# Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era[†]

*Christopher Soghoian*[‡]

## Abstract

Over the last few years, consumers, corporations and governments have rushed to move their data into "the cloud," adopting web-based applications and storage solutions provided by companies that include Amazon, Google, Microsoft and Yahoo.

Unfortunately the shift to cloud computing needlessly exposes users to privacy invasion and fraud by hackers. Cloud based services also leave end users vulnerable to significant invasions of privacy by the government, resulting in the evisceration of traditional Fourth Amendment protections of a person's private files and documents. These very real risks associated with the cloud computing model are not communicated to consumers, who are thus unable to make an informed decision when evaluating cloud based services.

This article will argue that the increased risk that users face from hackers is primarily a result of cost-motivated design decisions on the part of the cloud providers, who have repeatedly opted to forgo strong security solutions already used in other Internet based industries.

With regard to the intrusion upon user privacy performed by government agencies, fault for this privacy harm does not lie with the service providers; but the inherently coercive powers the government can flex at will. The third party doctrine, which enables government agents to obtain warrantless access to a suspect's private files stored by Internet service providers, is frequently criticized by privacy scholars. However, this article will argue that this doctrine becomes moot once encryption is in use and companies no longer have access to their customers' private data. The real threat to privacy lies with the fact that corporations can and have repeatedly been forced to modify their own products in ways that harm end user privacy, such as by circumventing encryption.

---



[‡] Ph.D. Candidate, School of Informatics and Computing, Indiana University. Email: csoghoian@gmail.com. Other research papers available at http://www.dubfire.net.

An earlier version of this article was presented to U.C. Berkeley's Privacy Law Scholars Conference. Thanks to Kevin Bankston, Fred Cate, Chris Hoofnagle, Marcia Hoffman, Rob Faris, Albert Gidari, Jennifer Granick, Orin Kerr, Susan Landau, Paul Ohm, Nicole Ozer, John Palfrey, Marc Rotenberg, Adam Shostack, Ryan Singel, Adam Thierer, Jonathan Zittrain as well several persons who asked to remain anonymous for their comments and suggestions.

This article was written while the author was a student fellow at the Berkman Center for Internet & Society at Harvard University. This article was started while the author was a technology policy intern at the American Civil Liberties Union of Northern California. This work was in part funded by Indiana University's Center for Applied Security Research and a Searle Freedom Trust Fellowship from the Institute for Humane Studies. The opinions expressed within, any mistakes and all omissions are the author's.

# Table of Contents

# I. Introduction

Over the last few years, consumers, corporations and governments have rushed to move their data to "the cloud,"[1] adopting web-based applications and storage solutions provided by companies that include Amazon, Google, Microsoft and Yahoo. Over 69% of Americans now use webmail services, store data online, or otherwise use software programs such as word processing applications whose functionality is in the cloud.[2] This trend is only going to continue, with industry analysts predicting that cloud computing related revenues will grow to somewhere between $40-$160 billion in over the next few years.[3]

Cloud computing services provide consumers with vast amounts of cheap, redundant storage and allow them to instantly access their data from a Web-connected computer anywhere in the world. Unfortunately the shift to cloud computing needlessly exposes users to privacy invasion and fraud by hackers. Cloud based services also leave end users vulnerable to significant invasions of privacy by the government, resulting in the evisceration of traditional Fourth Amendment protections of a person's private files and documents. These very real risks associated with the cloud computing model are not communicated to consumers, who are thus unable to make an informed decision when evaluating cloud based services.

This article will argue that the increased risks that users face from hackers are primarily a result of cost-motivated design tradeoffs on the part of the cloud providers, who have repeatedly opted to forgo strong security solutions. These vulnerabilities can easily be addressed through the adoption of industry standard encryption technologies, which are already in widespread use by online banks and retailers. Cloud providers should enable these encryption technologies, and more importantly, turn them on by default. This article will argue that the failure of cloud computing companies to provide these technologies is a strong indicator of a market failure. Fixing this may require user education in order to stimulate demand for safer solutions, or perhaps even the threat of government regulation.

With regard to the intrusion upon user privacy performed by government agencies, fault for this privacy harm does not lie with the service providers; but the inherently coercive powers which the government can flex at will. The third party doctrine, through which government agents can often obtain users' private files from service providers with a mere subpoena,[4] is frequently criticized by privacy scholars. However, this article will argue that this doctrine

---

[1] "Cloud Computing Services" involve "a software and server framework (usually based on virtualization)" that uses "many servers for a single software-as-a-service style application or to host many such applications on a few servers." See: "Perspectives on Cloud Computing and Standards," NIST, Information Technology Laboratory, *available at* http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf

[2] "Cloud Computing Gains in Currency," Internet and American Life Project, (Sep. 12, 2008), *available at* http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency.

[3] "Research firm IDC predicts cloud computing will reach $42 billion in 2012. (It defines the segment as "an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet.") Gartner Inc. projects world-wide cloud-services revenue will rise 21.3% in 2009 to $56.3 billion. (Gartner calls it "a style of computing where scalable and elastic IT-enabled capabilities are provided 'as a service' to external customers using Internet technologies"; its forecast includes online advertising.) Merrill Lynch last year estimated cloud-computing revenues would reach $160 billion in 2011. (Merrill declined to provide a copy of its report.)" Geoffrey A. Fowler and Ben Worthen, *The Internet Industry Is on a Cloud -- Whatever That May Mean*, THE WALL STREET JOURNAL, March 26, 2009, *available at* http://online.wsj.com/article/SB123802623665542725.html

[4] The government has long argued that an email is no longer in "electronic storage" once it has been read by the recipient, and thus it can be obtained using a subpoena with delayed notice. See 18 U.S.C.A. § 2703(b).

becomes moot once encryption is in use and companies no longer have access to their customers' private data. The real threat to privacy lies with the fact that corporations can and have repeatedly been forced to modify their own products in ways that harm end user privacy, such as by circumventing encryption.

Cloud computing providers are caught in an unenviable situation – since there is little they can do to guarantee their customers protection from the government's watchful gaze.[5] While on one hand, public interest groups and activists will criticize these companies for failing to protect their customers' privacy,[6] and on the other, the government can quietly force them to circumvent any privacy enhancing technologies that they do deploy.

This article is organized as follows. Part I introduces the concepts behind cloud computing, and the technical shifts that have made it possible for many users to unknowingly switch to cloud solutions. Part II will explore privacy and security related threats which users face from hackers, and the failure of service providers to protect users from them. Part III focuses on the trickier issue of intrusions by the government, and the ultimate inability of service providers to protect their users from these threats. Part IV concludes with policy recommendations, both legal and technical.

# I. Cloud computing

One of the defining characteristics of the personal computing paradigm is that users maintain physical control over their files and data. In fact, it was the departure from the mainframe computing model, in which users merely operated on slices of a central server's time and resources that marked the beginning of the personal computing era.

Personal computing users are able to make use of word processing programs such as Microsoft's Word in order to write memos, reports and letters, Microsoft's Excel and Intuit's Quicken in order to manage their finances and balance their books, and Apple's iPhoto, Adobe's Photoshop and other programs to organize, edit and catalog their digital photo collections.

This computing model has become firmly ingrained in the consciousness of consumers, and as such, we have become used to our documents, music, and photographs residing on our own personal devices as well as relying on our own computing resources to process and display our data. If we run out of storage space, or a task takes far too long, the solution is to upgrade our own computer – and likewise, if our computer suffers a hardware failure, is lost or stolen, we often lose our files.

In recent years, the computing industry has turned away from this personal computing model, and shifted towards online services, commonly described as "software as a service" or "cloud computing." This paradigm, in which the user's web-browser acts as a "thin client" and remote servers perform the majority of the data processing is rapidly being adopted by both consumers and businesses. As such, this model already plays a key role in the United States economy.[7]

---

[5] See generally, Albert Gidari Jr., Keynote Address: Companies Caught in the Middle, 41 U.S.F. L. Rev. 535, Spring 2007.

[6] For example, see: Electronic Privacy Information Center, *Complaint and Request for Injunction, Request for Investigation and for Other Relief, In the Matter of Google, Inc. and Cloud Computing Services*, March 17, 2009, *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf

[7] "Based on a survey of IT executives, CIOs, and other business leaders, IDC said this week it expects spending on IT cloud services to grow almost threefold in the next five years, reaching $42 billion by 2012" Roger Smith, *IDC Says IT Cloud Services To Reach*

The first application to move to the cloud was electronic mail – perhaps due to the fact that the use of the service already required Internet access. However, in time, other applications soon moved online. Google's Apps suite is the market leader in this area,[8] providing word processing, spreadsheets and presentation software functionality via a web browser. Microsoft, Adobe and Intuit have been quick to follow by releasing Web-based versions of their Office,[9] Photoshop[10] and Quicken products.[11]

Cloud computing enables a whole collection of computing resources such as applications, storage space and processing power to be delivered via the Internet. Hundreds of thousands of computers, located in data centers around the world handle the processing and storage of data for millions of individual users. The cloud computing model is deemed by many commentators to be the future of computing.[12]

Many firms wishing to draw attention to their own products have adopted and borrowed terms associated with "cloud computing," such as "Web 2.0", "software as a service" and other fashionable buzzwords. As a result, there is little agreement on the actual definition of "cloud computing."[13] For the purpose of this article, the term "cloud computing" will be used to apply to software offerings where the application is executed in a web browser, via software code that is downloaded (as needed) from a remote server that also stores users' files.[14]

### A. Benefits of cloud computing for service providers

The cloud computing model brings a number of important benefits to service providers: Reduced piracy, the ease of denying access to troublesome users, protection of sensitive technology and intellectual property, the ability to serve carefully targeted advertising to customers, and increased security.

The problem of unauthorized copying is almost non-existent when software is delivered via the web. This is because much of the computation occurs on the software provider's own servers. Since this code is never provided to the

---

*$42 Billion By 2012*, INFORMATION WEEK, October 20, 2008, *available at* http://www.informationweek.com/blog/main/archives/2008/10/idc_says_it_clo.html

[8] "This shows that Google's word processing and spreadsheet products have a noticeable lead over what may be its nearest rival, Zoho." Richard Macmanus, *Google Docs the Clear Leader in Web Office Market*, READWRITEWEB, December 7, 2007, *available at* http://www.readwriteweb.com/archives/google_docs_web_office_leader.php

[9] *See generally*: Microsoft Office Live, http://www.officelive.com/

[10] *See generally:* Photoshop Express, https://www.photoshop.com/express/landing.html

[11] *See generally*: Quicken Online, http://quicken.intuit.com/

[12] "Pretty much everyone in the tech industry agrees it's the future—including Microsoft, which last week devoted much of its annual conference for developers to a rollout of new cloud technologies and a pep talk about why customers should jump aboard." Daniel Lyons, *Today's Forecast: Cloudy*, NEWSWEEK, November 1, 2008, *available at* http://www.newsweek.com/id/166818

[13] "While almost everybody in the tech industry seems to have a cloud-themed project, few agree on the term's definition." Geoffrey A. Fowler and Ben Worthen, *The Internet Industry Is on a Cloud -- Whatever That May Mean*, THE WALL STREET JOURNAL, March 26, 2009, *available at* http://online.wsj.com/article/SB123802623665542725.html

[14] While pure remote storage or computing services such as Amazon's S3 are commonly described as cloud services, they are beyond the scope of this article.

user, it cannot be copied. Thus, while thousands of users illegally share copies of Microsoft Office and Adobe Photoshop via online peer to peer filesharing services[15], the code powering Google's Docs and Adobe's Photoshop Express cloud based products remains under tight wraps. Users are free to sign up for and use these tools, but they (as well as the firms' competitors) are unable to host the tools on their own servers.

Another benefit of cloud computing is the ability to easily terminate access to particular users. Software providers are able to maintain control over access to their services, often via a unique account and password per customer. If a company wishes to cut off access to a particular customer, this can be done by simply suspending an individual account.

Furthermore, cloud computing makes it far easier to protect trade secrets. For example, companies like Adobe whose flagship Photoshop product contains proprietary image-altering algorithms may wish to keep such technology secret from their competition. Whereas previously, a competitor could purchase a copy of Photoshop, run it on a desktop computer, and reverse engineer the product's key algorithms.[16] Under the cloud computing paradigm, the user's Web browser submits an image to Adobe's servers, which apply the algorithm, and then return the modified image. Since the secret algorithm is never executed on the user's computer, reverse engineering is made exceedingly difficult.

Cloud services also allow software vendors to easily embed advertisements into their offerings, and to use sophisticated data mining algorithms to display advertisements related to the users' private data held within the cloud.[17]

Finally, cloud computing providers can be certain that end users are always running the most up-to-date version of their software, a problem that has plagued the traditional PC industry. Cloud vendors can apply the fix to their own servers, without requiring that users choose to update it themselves. This ability to roll out instant updates across an entire product line reduces tech support costs, and helps to protect the company's reputation from being damaged by claims of shoddy workmanship or poor security practices.

### B. Benefits of cloud computing for end-users

For the consumers and businesses that have switched to cloud based services, there are a number of benefits including price, reliability, accessibility as well as the ease of access independent of a specific computer.

---

[15] See for example, the undertaker, *Microsoft Office 2007 Complete Version + CD Keys,* The Pirate Bay, May 12, 2008, available at http://thepiratebay.org/torrent/4183909/Microsoft_Office_2007_Complete_Version___CD_Keys. TheFinder, *Adobe Photoshop CS3 Extended + Crack*, The Pirate Bay, January 08, 2008, *available at* http://thepiratebay.org/torrent/3967056/Adobe_Photoshop__CS3__Extended___Crack.

[16] Reverse Engineering is generally defined as the process of "starting with the known product and working backward to divine the process which aided in its development or manufacture." See: *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974). See also: Pam Samuelson, The Law and Economics of Reverse Engineering, 111 Yale L.J. 1575 (2002) *available at* http://www.yalelawjournal.org/pdf/111-7/SamuelsonFINAL.pdf

[17] "All major free webmail services carry advertising, and most of it is irrelevant to the people who see it. Some services which compete with Gmail attempt to target theirs ads to users based on their demographic profile (e.g., gender, income level or family status). Google believes that showing relevant advertising offers more value to users than displaying random pop-ups or untargeted banner ads. In Gmail, users will see text ads and links to related pages that are relevant to the content of their messages." More on Gmail and Privacy, January, 2007, available at http://mail.google.com/mail/help/about_privacy.html.

Most cloud computing services are either free or significantly cheaper than more traditional desktop offerings.[18] Consumer orientated services are generally "free," in so far as users do not pay money for access, but instead submit to behavioral advertising and data mining of their activities, social networks and communications.[19] Commercial editions of cloud services often come at a direct financial cost, but one which is far less than comparable desktop software. Of course, Microsoft Office and Google Docs are not equal in features, but Google's product suite is often *good enough* for school work, as well as the simple word processing and spreadsheet tasks performed by many employees.[20]

Many of the cloud based services include built-in revision control systems,[21] which enable a user to immediately access past versions of a document. Files are automatically backed up, at regular intervals, and stored on multiple servers around the country. As a result, hardware failure in the user's computer will not result in the loss of any data.[22] Furthermore, in the event that the user suffers a hardware failure, they merely need to open a web-browser on a different computer, and can then continue editing their documents where they had previously left off.

Since the applications and user's files are stored online, they are accessible from anywhere in the world. A user can sit down at a new computer (even miles from their home) and instantly access a copy of her documents. Furthermore, since most of the heavy duty processing is performed by remote servers and not by the user's computer, cloud computing extends the usable life of older computer hardware as well as providing data access to less powerful devices such as mobile phones.

### C. Cloud creep and the rise of cloud services as the pre-installed default

While some users may choose to switch to cloud based services, others are not as fortunate and often this decision is made without their knowledge.

Due to the significant reductions in licensing and support costs, many corporate and government IT managers are making the switch. Compared to the $500 list price for the full version of Microsoft Office Professional[23], Google's

---

[18] "[Google] Premier Edition's yearly price of $50 per user appears to be less than half the $122 we believe enterprises are currently spending for e-mail with much more stringent storage limitations." Tom Austin, Matthew W. Cain and Michael A. Silver, *Google Targets Enterprise E-Mail and Collaboration Tools*, Gartner Research Report, 27 February 2007, *available at* http://www.gartner.com/DisplayDocument?doc_cd=146730&ref=g_rss

[19] See generally: Grant Yang, *Stop the Abuse of Gmail*, 2005 Duke L. & Tech. Rev. 0014, *available at* http://www.law.duke.edu/journals/dltr/articles/pdf/2005dltr0014.pdf

[20] "So who might want Google Apps in its current form? Well, there are certainly scads of workers in the world who really only need basic tools." Harry McCracken, *Google Apps vs. Microsoft Office*, PC WORLD, February 22, 2007, *available at* http://blogs.pcworld.com/techlog/archives/003783.html

[21] "Revision control …. is the management of changes to documents, programs, and other information stored as computer files." See: http://en.wikipedia.org/wiki/Revision_control

[22] "Safely store your work. Online storage and auto-save mean you needn't fear local hard drive failures or power outages." Google Docs Tour, http://www.google.com/google-d-s/tour3.html.

[23] Buy Microsoft Office Professional 2007, Microsoft Online Store, http://office.microsoft.com/en-us/suites/FX102434861033.aspx

$50-per-year price tag is a bargain – especially given that it includes telephone, e-mail and web support.[24] Corporate enterprise managers are able to re-brand the Google Apps products with their own companies' logos. The services also plug directly into existing IT infrastructure. For example, corporate Google Mail customers can configure the service to use their own Internet domain names, making the switch oblivious to outsiders and customers who might otherwise recognize the telltale 'gmail.com' email addresses.

Incoming students at thousands of universities are now issued Google accounts on their first day, enabling them to write term papers and access their official school email inboxes that are hosted on Google's servers.[25] University students are not alone in this switch – before he was tapped to become the Federal Chief Information Officer, Vivek Kundra switched 38,000 Washington DC employees from Microsoft Office to Google Docs.[26] Google claims that nearly 2 million businesses use Google Apps, with thousands more signing up each day.[27]

While some students and employees realize that they are using cloud based services, many others may not, particularly when the services have been rebranded and heavily stripped of Google's logos.[28]

At the consumer level, cloud services are also making inroads through the use of pre-installed desktop icons on new PCs, particularly in low end devices. Over the past year, sub $400 "netbook" portable computers have taken the computing industry by storm. The manufacturers of these devices operate with extremely low profit margins, which they hope to make up in volume.[29] As a result, the netbook makers are trying many possible ways to lower their own costs. One of the main ways they have done this to abandon Microsoft's operating system and Office suite. In

---

[24] "Google Apps Premier Edition, Education Edition, and Authorized Reseller customers have access to a phone line to report a service unusable issue." About Phone Support, July 27, 2009, available at http://www.google.com/support/a/bin/answer.py?hl=en&answer=65260

[25] "As of this fall, over five million students at thousands of schools in more than 145 countries have "gone Google" and are actively using Google Apps Education Edition on campus." Miriam Schneider and Jason Cook, Five million students going back to school are "going Google", post to Official Google Blog, September 8, 2009, available at http://googleblog.blogspot.com/2009/09/five-million-students-going-back-to.html. "Thousands of colleges, including USC and Notre Dame, and nearly 2 million businesses have adopted Google Apps, the company says. Most schools and small businesses get Google Apps for free, but the company has also converted some heavy corporate hitters into paying customers, including biotech company Genentech, electronics maker Motorola and chip maker Fairchild Semiconductor." David Sarno, *Los Angeles City Hall becomes tech giants' battlefield*, LOS ANGELES TIMES, September 28, 2009, *available at* http://www.latimes.com/business/la-fi-email-wars28-2009sep28,0,6817066,full.story.

[26] "The 34-year-old city technology chief signed a contract worth almost $500,000 a year in June for all 38,000 municipal employees to use Google's e-mail, spreadsheet and word- processing programs, giving them an Internet-based alternative to Microsoft Corp.'s Office software, installed on computers. Accountants, teachers and firefighters use Google to set budgets, track truancy rates and map emergency routes." Molly Peterson, *Google Rewires Washington in Challenge to Microsoft*, BLOOMBERG, October 10, 2008, *available at* http://www.bloomberg.com/apps/news?pid=20601109&sid=a8q7UONag9nA

[27] See: above quote from Sarno.

[28] Users of the Google Apps suite see a small "powered by Google" logo in the bottom of each page. All other branding is that of the company subscribing to the service.

[29] "Acer expects to sell 12-13 million netbooks in 2009, and ASUS expects to sell roughly 7 million netbooks …. The total would put netbook shipments over 20 million in 2009 from just the two companies, some 50% more than 2008's 14 million sold. If Acer and ASUS retain a percentage of their total market share from Q3 2008, shipments of netbooks in 2009 could top 30 million units, doubling 2008's total." Ari Allyn-Feuer, *ASUS, Acer: strong netbook sales in '09*. Is 30M possible?, ARS TECHNICA, January 7, 2009, *available at* http://arstechnica.com/hardware/news/2009/01/asus-acer-strong-netbook-sales-in-09-is-30m-possible.ars

addition to pre-installing these computers with the Linux operating system, several manufacturers also ship their netbook products with prominent icons for Google's Docs and Spreadsheets tools.[30]

In addition to the general industry trends that are pushing many towards cloud based services, new technologies make such transitions less obvious to end-users. Two of these are now highlighted: single site browsers, and offline content.

### D. Single site browsers

The shift to cloud computing moved much of a user's normal activity to the Web browser. While this certainly lowers many barriers to user adoption, such as negating the need to download and install specific applications, this transition also raises a number of security and usability issues. For example, Web browsers generally store all of a user's saved passwords, browsing history and other sensitive information in a single place. As such it is possible for malicious websites to exploit browser vulnerabilities in order to steal information associated with other existing or previous browsing sessions – such as a logged in email account or online banking session.[31] It is for this reason that some security experts recommend that consumers use one web browser for general surfing, and another for more sensitive tasks, such as online banking.[32]

Seeking to mitigate these risks, Web browser vendors have released single site browser technology, the most advanced of which is Mozilla's Prism tool for its Firefox platform.[33] Prism and the other single site browsers allow a user to "split web applications out of the browser and run them directly on the desktop."[34] A Prism user can create a dedicated icon on their desktop for any Web site they regularly visit. When that icon is clicked, a dedicated browser window will open taking them to the pre-assigned Web site. Each Prism instance maintains its own profile for

---

[30] "The system's applications include such usual Linux favorites as OpenOffice, Firefox, and Thunderbird. To make life easier still, some pages include links to useful sites such as Google Docs." -- Describing the Xandros Linux distribution pre-installed by default on many ASUS EEE netbook computers. Steven J. Vaughan-Nichols, *Linux-powered Asus Eee PC mini-laptop arrives*. November 1, 2007, *available at* http://www.desktoplinux.com/news/NS5557994061.html

[31] "[A]ttackers could compromise a Gmail account--using a cross-site scripting vulnerability--if the victim is logged in and clicks on a malicious link." Liam Tung, *Gmail cookie vulnerability exposes user's privacy*, CNET NEWS, September 27, 2007, *available at* http://news.cnet.com/Gmail-cookie-vulnerability-exposes-users-privacy/2100-1002_3-6210353.html. "Security researcher Petko Petkov has revealed a cross-site request forgery vulnerability in Gmail that makes it possible for a malicious web site to surreptitiously add a filter to a user's Gmail account that forwards e-mail to a third-party address." Ryan Paul, *Serious cross-site request forgery vulnerability found in Gmail*, ARS TECHNICA, September 27, 2007, *available at* http://arstechnica.com/software/news/2007/09/cross-site-request-forgery-vulnerability-found-in-gmail.ars "Researchers from Princeton University today revealed their discovery of four major Websites susceptible to the silent-but-deadly cross-site request forgery (CSRF) attack -- including one on ING Direct.com's site that would let an attacker transfer money out of a victim's bank account …. The CSRF bug they found on ING's site would have let an attacker move funds from the victim's account to another account the attacker opened in the user's name, unbeknownst to the user. Even using an SSL session wouldn't *protect* the user from such an attack" Kelly Jackson Higgins, *CSRF Flaws Found on Major Websites*, DARK READING, September 29, 2008, *available at* http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=211201247

[32] See generally: Rich Mogull, *Making the Move to Multiple Browsers*, Post to Securosis blog, June 3, 2008, *available at* http://securosis.ehclients.com/blog/making-the-move-to-multiple-browsers

[33] See generally, Mozilla Prism: http://labs.mozilla.com/projects/prism/, See also Fluid for Apple's Safari web browser: http://fluidapp.com/

[34] See *Introducing Prism*, post to Mozilla Labs blog, October 24, 2007, *available at* http://labs.mozilla.com/2007/10/prism/.

browser preferences and user data, and each Prism application also runs as its own system process. The end result is that a malicious website accessed from one Prism session (or a Firefox browser window) is unable to access any of the private data associated with another Prism application.

In addition to these security benefits, Prism brings several changes to the user interface. By default, Prism applications do not show any of the browser's traditional branding. The web site address of the current page is not displayed, there are no forward, back or refresh buttons, nor is there any way to see when the user is or isn't connecting via a secure, encrypted connection.[35]

While operating system vendors and corporate IT managers are already installing links to cloud based services on user's desktops, Prism and other Single Site Browser technologies make this process even easier[36]. Particularly for end-users as yet unfamiliar with Web-based word processing and office tools, Prism can make these sites seem like regular applications, and make it possible to ignore the fact that the services are Internet based at all.

### E. Offline content

As applications first started to move into the cloud, one of the few obvious disadvantages was that users had to be connected to the Internet in order to access their documents and personal files. When on an airplane, or in a public place without wireless Internet access, users found themselves unable to access files that would have traditionally been just a few clicks away.

Google was the first major provider to try and address this issue through the release of its Gears browser add-on tool in 2007.[37] This software extension provides a standard application programming interface (API) that websites can use to enable offline data storage and access. Within months of the release, Google added offline support via Gears to its Reader, Docs, Spreadsheets and Gmail products.[38] Thus, with Gears installed, a Gmail user can have almost complete access to their inbox and draft new emails when away from an Internet connection. Once a connection is re-established, the browser automatically synchronizes with Google's servers, sending the stored messages and downloading those newly received.

---

[35] "Personal computing is currently in a state of transition. While traditionally users have interacted mostly with desktop applications, more and more of them are using web applications. But the latter often fit awkwardly into the document-centric interface of web browsers. And they are surrounded with controls–like back and forward buttons and a location bar–that have nothing to do with interacting with the application itself." *Introducing Prism*, post to Mozilla Labs blog, October 24, 2007, *available at* http://labs.mozilla.com/2007/10/prism/.

[36] "Jolicloud is a custom Linux distribution that is designed specifically for netbook devices. It uses Mozilla's Prism Web runtime and Canonical's Ubuntu Netbook Remix (UNR) to deliver a Web-centric Linux environment that is easy to use." Ryan Paul, *Hands-on with an alpha of the Jolicloud netbook distro*, ARS TECHNICA, July 27, 2009, *available at* http://arstechnica.com/open-source/reviews/2009/07/hands-on-jolicloud-alpha-combines-ubuntu-and-mozilla-prism.ars.

[37] *Google Launches Gears Open Source Project to Bring Offline Capabilities to Web Applications*, Press Release, May 31, 2007, *available at* http://www.google.com/intl/en/press/pressrel/gears_20070530.html

[38] See generally: Jacqui Cheng, *Google Docs pulls head out of the cloud, goes offline*, ARS TECHNICA, March 31, 2008, *available at* http://arstechnica.com/old/content/2008/03/google-docs-pulls-head-out-of-the-cloud-goes-offline.ars. See also David Chartier, *Gmail finally gets offline access—with caveats*, ARS TECHNICA, January 28, 2009, *available at* http://arstechnica.com/web/news/2009/01/gmail-finally-gets-offline-accesswith-caveats.ars

While Google's Gears was the first offline web content API to be released, other companies such as Yahoo and Adobe have since released similar products.[39] In 2008, an open-standard for offline content was added to the next generation HTML 5 specification, support for which was quickly adopted by practically all of the non-Microsoft web browsers.[40] Thus, the latest versions of Firefox and Apple's now include support for this technology,[41] enabling web site designers to add offline data functionality to their sites without requiring the user to download and install any additional software.

## F. Confusion

The mass deployment of cloud based services, particularly when coupled with single site browser and offline content technology will likely lead to a significant risk of confusion for end users. As computer manufacturers, employers and universities deploy cloud based tools on the desktop, many users may fail to realize that they are in fact using an Internet based service. This risk of confusion will likely increase when cloud based applications lack any recognizable browser branding, and continue to function when the user is not connected to the Internet.

In the not too distant future, a non-expert user will sit down at a new computer (perhaps provided to them by an employer or purchased at a store), click on the "Word Processor" link on the computer's desktop, and will begin typing a document. The application will appear similar to other word processors but will actually be a sophisticated Web application running in a cloaked Web browser. This shift to a Web based technology will be accompanied by a radical shift in the user's rights and "expectation of privacy," at least as interpreted by the courts; even if the user herself does not realize that her documents are ever leaving her computer. Many users will be completely unaware that this shift has occurred, at least until it is too late.

---

[39] "The first real fruits of Yahoo's $350 million acquisition of Zimbra are becoming apparent with the release Thursday of the Yahoo Zimbra Desktop. The e-mail software, available as a free download for Windows and Mac, works when the user is offline, and it offers options for basic online word processing and spreadsheets, task management, and file storage." Stephen Shankland, *Zimbra Desktop gives Yahoo Mail offline access*, CNET NEWS, July 24, 2008, *available at* http://news.cnet.com/8301-1023_3-9998418-93.html. "One of the greatest abilities of AIR, in my opinion, is the ability to create an application to run online and offline. The application could allow the user to make changes to their account, content, etc. while not connected and sync the data online when the connection returns. The user will only love the application even more." John C. Bland II, *Taking Adobe AIR Applications Offline*, Adobe Labs, April 24, 2007, *available at* http://labs.adobe.com/wiki/index.php/AIR:Articles:Taking_Apollo_Applications_Offline

[40] If Mozilla, Opera and Apple's Safari browser have their way, the HTML specification could be getting its first major point update in a decade. The three vendors have banded together in a proposal to the W3C for the HTML 5 specification, which includes Web Apps 1.0 and Web Forms 2.0 specifications and that it's also backwards compatible with HTML 4 … HTML is the foundation markup language on which the Web was and is built and was originally created by Tim Berners-Lee. The last major upgrade to HTML was in 1997 with the release of version 4.0." Sean Michael Kerner, *Is The Web Ready For HTML5?*, InternetNews.com, April 16, 2007, *available at* http://www.internetnews.com/xSP/article.php/3672011.

[41] "The current working spec for the HTML5 standard has a lot of exciting features we would eventually like to implement in WebKit. One feature we felt was exciting enough to tackle now even though the spec is still in flux is client-side database storage." Brady Eidson, *WebKit Does HTML5 Client-side Database Storage*, Surfin' Safari Blog, October 19, 2007, *available at* http://webkit.org/blog/126/webkit-does-html5-client-side-database-storage/. "Firefox 3.5 supports the HTML 5 specification for offline caching of web applications' resources" *Offline resources in Firefox,* available at https://developer.mozilla.org/en/Offline_resources_in_Firefox.

## II. Many cloud computing services are needlessly vulnerable to hackers

The vast majority of cloud computing services are, by default, insecure.[42] Often, usernames and passwords are transmitted to remote servers via unencrypted network connections. In cases where encryption is used, it is typically only used to transmit the initial login information, while all subsequent data is sent *in the clear*.[43] This data can easily be snooped on by hackers. This exposes users to significant risks when they connect to the services using public wireless networks.[44] These flaws are rarely if ever disclosed to end-users.[45]

In order to explore the issues surrounding these privacy risks, consider the following two scenarios:

Alice, a college student, decides to do her homework at a coffee shop, using her laptop and a copy of Microsoft Word. In such a situation, it will be exceedingly difficult for a malicious person (perhaps sitting at another table or across the street) to breach her privacy. If the evil-doer is sitting behind her, he could perhaps read over Alice's shoulder, but such activity would soon become obvious. If he is extremely tech savvy, perhaps he can hack into Alice's computer over the wireless network – but this will require that Alice's operating system be vulnerable to an attack for which no patches have been released by the software vendor, or which Alice has not yet applied. Such an attack will also require that the adversary perform the *active* task of breaking into Alice computer in order to steal a copy of her documents.

Compare this to a similar situation in which Alice is using Google Docs on her laptop, at the same coffee shop. In this case, every character that Alice types into her word processing document is transmitted to Google's remote servers over the unsecured wireless network.[46] Due to the fact that Google's services do not by default use encryption to

---

[42] "A majority of the large Web-based email services, for example, encrypt the login process, but not the contents of email messages. Anyone along the path between the user and the service's data center could intercept this information, opening users to privacy and security risks." Predrag Klasnja *et al*, *"When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use*, In CHI '09: Proceedings of the 27th international conference on Human factors in computing systems (2009), pp. 1993-2002, *available at* http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf. "Google is not the only Web 2.0 firm which leaves its customers vulnerable to data theft and account hijacking. Users of Microsoft Hotmail, Yahoo Mail, Facebook and MySpace are also vulnerable to these attacks. Jacob Appelbaum et al, *Re: Ensuring adequate security in Google's cloud based services*, Open Letter to Google CEO Eric Schmidt, June 16, 2009, *available at* http://www.cloudprivacy.net/letter/.

[43] "'In the clear' is a term of art which means without encryption." Paul Ohm, Good Enough Privacy, 2008 University of Chicago Legal Forum. (citing Neil Daswani, Christoph Kern, and Anita Kesavan, Foundations of Security: What Every Programmer Needs to Know (Apress 2007)).

[44] "[T]he broadcast nature of Wi-Fi means that anyone within range of the network can receive and potentially read transmissions intended for any other device on the network.", Predrag Klasnja *et al*, *"When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use*, In CHI '09: Proceedings of the 27th international conference on Human factors in computing systems (2009), pp. 1993-2002, *available at* http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf "

[45] Despite living in a technologically sophisticated area of the U.S., the participants were not aware that information sent over Wi-Fi could be seen by others." Predrag Klasnja *et al*, *"When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use*, In CHI '09: Proceedings of the 27th international conference on Human factors in computing systems (2009), pp. 1993-2002, *available at* http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf "

[46] In some cases, this happens in real-time, in order for features like spell-check to work. In others, documents will be automatically saved to a remote server at regular intervals.

transmit user data, the attacker can use one of many off-the-shelf tools to *passively* "sniff" the network and capture Alice's private data as it is transmitted to the company's servers. Worse, the hacker can capture the credentials necessary to later impersonate Alice, thus enabling him to later connect to her account and browse through older documents and emails.[47]

Freely available off the shelf tools automate these widely publicized vulnerabilities in many cloud computing services.[48] These tools abstract away the technical details underpinning the data capture techniques, and since they allow the attacks to be performed with a few mouse clicks, are accessible to even non-expert evil doers. While the service providers have known about these flaws (and the ease with which they can be exploited) for several years,[49] the service providers continue to ship products with unsafe default settings,[50] and in most cases, do not offer any protection to end users.[51]

Users of cloud computing services lack basic security protections which users of traditional PC based software often take for granted. Google, the market leader, and nearly all other leading cloud providers offer products that are by

---

[47] "While Web 2.0 services like Gmail and Facebook encrypt usernames and passwords that users submit when they log into their accounts, all keep tabs on users by placing a "cookie," or tiny text file, on the user's computer. Those cookie files are not encrypted, which means that anyone who is monitoring the network traffic flowing over a wireless network can simply intercept one of those cookie files. This allows an attacker to log in as the victim, effectively cloning the account without knowledge of the victim's login credentials." Brian Krebs, *New Tool Automates Webmail Account Hijacks*, THE WASHINGTON POST -- Security Fix blog, August 2, 2007, *available at* http://blog.washingtonpost.com/securityfix/2007/08/new_tool_automates_webmail_acc.html

[48] "It turns out an adversary able to position themselves in between you and a website is able to inject arbitrary http-based content elements for domains that do not set the 'Encrypted Sessions Only' property of their cookies, and thus cause your client to transmit these cookies via clear text, intercept them, and impersonate you. " Mike Perry, *Automated HTTPS Cookie Hijacking*, August 14, 2009, *available at* http://fscked.org/blog/fully-automated-active-https-cookie-hijacking. Code available at http://code.google.com/p/cookiemonster/ See also: " This tool …. will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial." Moxie Marlinspike, *SSLStrip*, *available at* http://www.thoughtcrime.org/software/sslstrip/. See also: Robert Graham, *Sidejacking with Hamster*, August 5, 2007, http://erratasec.blogspot.com/2007/08/sidejacking-with-hamster_05.html, *tool available for download at* http://www.erratasec.com/sidejacking.zip

[49] "I described this attack in detail in a post to BugTraq and notified Google a year ago, but unfortunately, my announcement was largely overshadowed by Robert Graham's 'SideJacking' demonstration at Black Hat. His tool was simply a sniffer that just gathered cookies for sites as users on the local network visited them. The attack I described was much more flexible, much more powerful, and just as automated, but without a tool and a demonstration to back up my claims, nobody listened." Mike Perry, *Automated HTTPS Cookie Hijacking*, August 14, 2009, *available at* http://fscked.org/blog/fully-automated-active-https-cookie-hijacking

[50] "Default settings are pre-selected options chosen by the manufacturer or the software developer. The software adopts these default settings unless the user affirmatively chooses an alternative option." Kesan, Jay P. and Shah, Rajiv C., *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, Notre Dame Law Review, Vol. 82, pp. 583-634, 2006.

[51] "Hotmail, Yahoo Mail, and Facebook … remain vulnerable to a so-called "man-in-the-middle attack" in which someone on the same Wi-Fi network hijacks the session cookies that are transmitted between a user's browser and a Web site." Elinor Mills, *Google making SSL changes, other sites quiet*, CNET NEWS, August 22, 2008, *available at* http://news.cnet.com/8301-1009_3-10023958-83.html

default vulnerable to snooping, account hijacking, and data theft by third parties.[52] Every time a user logs into their Google Mail, Docs, Flickr, Facebook or MySpace account from a coffee shop or other public wireless network, they risk having their private data stolen by hackers.

This problem is not due to the Web based nature of these services. Consumers are able to safely check their online bank accounts, order books from Amazon, or trade stocks with an online broker while using open wireless networks without any risk of account hijacking or data theft. Yet this private and valuable information flows over the same Internet connection that Google, Facebook and MySpace have somehow been unable (or unwilling) to secure.

### A. The benefits of network encryption

Bank of America, American Express and Amazon[53] all use the industry standard Hypertext Transfer Protocol Secure (HTTPS) encryption protocol to insure that all customer information is securely transmitted over the network.[54] This technology enables a user to safely conduct business online, without the risk of a hacker capturing her private data as it crosses the network. This is because to third parties, her encrypted communications appear as undecipherable gibberish.

Most cloud based services transmit nearly every single bit of a user's data to the service's central servers over the network in the clear. In some cases, this even includes the username and password used to login to the user's account, significantly raising the risk of account theft.[55] This information can be captured with one of many off the shelf tools known as "packet sniffers." Some operating systems, such as Linux and Apple's Mac OS even include these data capture tools out of the box.[56]

While most cloud services do not offer any encryption at all, Google does at least offer HTTPS encryption for many of its services. However, it does so as an unadvertised option, which is disabled by default.[57] Other cloud providers such

---

[52] Adobe's Photoshop Express is a rare exception to the norm. This service is only available via a secure SSL encrypted session. See for example, http://www.photoshop.com/ which automatically redirects to the secure https://www.photoshop.com.

[53] "Amazon encrypts communications related to payment but not purchase history and recommendations, according to Perry. An Amazon spokeswoman said the company does not comment on security measures." Elinor Mills, *Google making SSL changes, other sites quiet*, CNET NEWS, August 22, 2008, *available at* http://news.cnet.com/8301-1009_3-10023958-83.html

[54] In fact, it is impossible to connect to the web sites of both Bank of America and American Express using anything *but* an encrypted session. For example, typing http://www.americanexpress.com automatically redirects the user's browser to https://www.americanexpress.com. Likewise, visiting http://www.bankofamerica.com immediately redirects to https://www.bankofamerica.com.

[55] For example, MySpace users send their usernames and passwords to the site over an unencrypted connection.

[56] Both Mac OS and most Linux distributions include tcpdump. This tool is not particularly easy to use, and so many users opt for the far more user friendly 'Wireshark.'

[57] Users of Google's services can enable security on a case-by-case basis by connecting to a different URL for the various Google services. Rather than connecting to http://mail.google.com, users must connect to https://mail.google.com. Due to the fact that web browsers default to http (if nothing else is specified), a user who simply types "mail.google.com" into her web browser will have her communications sent over the network without any encryption.

In 2008, more than a year after Google was first notified about attackers in which its customers account authentication tokens could be hijacked, the company released a new feature to enable automatic encryption for Gmail. See: http://gmailblog.blogspot.com/2008/07/making-security-easier.html

as Yahoo and Facebook do not offer HTTPS protection for their customer's communications. Even if a user of these services wishes to protect herself from third party snoopers, there is nothing that she can do. Of course, Facebook, Yahoo and Microsoft *could* offer HTTPS. Likewise, they and Google could even turn it on *by default*, so that all users are automatically protected from all passive data theft.

Contrast this to the security of online banks – consumers don't have to go out of their way to login to the "secure" front-end to their bank's website. They don't have to manually enter a different URL, or select a hidden configuration option. Consumers simply go to the bank's website, and login. Everything else is taken care of for them.

### B. Why do cloud providers opt to leave users exposed?

HTTPS is a technical standard which is supported by every modern web browser and every popular web server.[58] The free open-source Apache web-server, which powers most popular websites,[59] includes HTTPS support by default.

In 2007, Google's poor security defaults were the subject of some tech media coverage, primarily due to the release of tools that automated the theft of data from Google customers' accounts. Defending the company's decision to not enable HTTPS encryption by default, a Google spokesperson stated then that:

> "We use [HTTPS encryption] to protect your password every time you log into Gmail, but we don't use [HTTPS encryption] once you're in your mail unless you ask for it …. Why not? Because the downside is that [HTTPS encryption] can make your mail slower. Your computer has to do extra work to decrypt all that data, and encrypted data doesn't travel across the internet as efficiently as unencrypted data. That's why we leave the choice up to you."[60]

For encryption to be a "choice", Google's customers would need to receive notice of the risks if they do not seek out this unadvertised option.[61] The company does not provide its customers with this information, and so it is unlikely that most users would believe that the issue of encryption protection for email is something they have decided. However, while the company argues that this issue is one of choice, the company has forced encryption (with no option to turn it off) for users of some of its other products.

Google's Health service enables users to browse through and manage their private health information online. Google's Voice service lets customers initiate VOIP phone calls, send text messages, and manage voicemail inboxes.

---

The company's help page for the encryption preference notes that "If you sign in to Gmail via a non-secure Internet connection, like a public wireless or non-encrypted network, your Google account may be more vulnerable to hijacking. Non-secure networks make it easier for someone to impersonate you and gain full access to your Google account, including any sensitive data it may contain like bank statements or online log-in credentials. We recommend selecting the 'Always use https' option in Gmail any time your network may be non-secure." See: http://mail.google.com/support/bin/answer.py?hl=en&ctx=mail&answer=74765

[58] See: The Transport Layer Security (TLS) Protocol Version 1.2, http://tools.ietf.org/html/rfc5246

[59] Apache is used by more than 50% of the servers on the web. http://news.netcraft.com/archives/2009/01/16/january_2009_web_server_survey.html

[60] Ariel Rideout, *Making Security Easier*, Post to the Official Gmail Blog, July 24, 2008, *available at* http://gmailblog.blogspot.com/2008/07/making-security-easier.html

[61] "Google currently does very little to educate its users, and the sparse information describing encryption options is hidden, and presented in terms that few members of the general public will understand." Jacob Appelbaum et al, *Re: Ensuring adequate security in Google's cloud based services*, Open Letter to Google CEO Eric Schmidt, June 16, 2009, *available at* http://www.cloudprivacy.net/letter/.

However, unlike with its Gmail, Docs, and Calendar products, Google only provides access to Health and Voice via HTTPS encrypted communications sessions, recognizing the highly sensitive health and call record information users entrust to Google. Likewise, Google's AdWords and AdSense products, which form the backbone of Google's advertising business, can only be managed by customers using a secure HTTPS connection.

Even if companies genuinely wish to offer their users a choice over the ability to enable or disable encryption, the default option is critical, since so few people will ever modify it.[62] Furthermore, while the importance of safe defaults has been widely documented by scholars in the fields of computer science, economics and law, many companies still opt for unsafe defaults, and instead blame users for not seeking out and enabling those options.[63]

A far more likely reason why Google has not offered HTTPS encryption by default and other companies have opted to forgo HTTPS completely is the issue of cost. Simply put, providing a HTTPS encrypted connection takes significantly more processing power and memory for a Web server to provide than a "normal" web connection. For example, if a common Web server can normally process 30,000 simultaneous connections, it might only be able to handle 5,000 simultaneous SSL encrypted connections.[64] Thus, enabling HTTPS by default will significantly increase the cost of providing services to end-users, simply due to the massive increase in the number of servers required to handle and process all of those encrypted connections.

---

[62] "The defaults turn out to be crucially important, because few users go to the trouble of adjusting the settings. Asked how many members ever change a privacy setting, [Facebook's Chief Privacy Officer Chris] Kelly said 20 percent." Randall Stross, *When Everyone's a Friend, Is Anything Private?*, March 7, 2009, *available at* http://www.nytimes.com/2009/03/08/business/08digi.html. "A Pew Internet & American Life Project study from August 2000 found that 84% of Internet users in the United States were concerned about businesses and strangers getting their personal data online. However, 56% did not know about cookies. More notably, 10% said they took steps to block cookies from their PCs. However, a study by Web Side Story found the cookie rejection rate was less than 1%. These data show that while people were concerned about their online privacy, they were unaware of the most significant technology that affects online privacy. While a small proportion of these people claimed to have changed the default setting, the data actually show that a very small percentage, less than 1%, actually change the default setting. In sum, despite the overwhelming concern for privacy, almost everyone deferred to the default setting and accepted cookies." Kesan, Jay P. and Shah, Rajiv C., *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, Notre Dame Law Review, Vol. 82, pp. 583-634, 2006. "Default options have an enormous impact on household 'choices.' Such effects are documented in the literature on 401(k) plans. Defaults affect 401(k) participation, savings rates, rollovers, and asset allocation. For example, when employees are automatically enrolled in their 401(k) plan, only a tiny fraction opt out, producing nearly 100% enrollment. But when employees are not automatically enrolled, less than half enroll on their own during their first year of employment." James J. Choi et al, *Optimal Defaults*, The American Economic Review, Vol. 93, No. 2, Papers and Proceedings of the One Hundred Fifteenth Annual Meeting of the American Economic Association, Washington, DC, January 3-5, 2003 (May, 2003), pp. 180-185.

[63] "Facebook appears to have a strategy of dumping all the really hard security decisions on the users -- so that they can respond to criticism by blaming users for not turning off features X and Y. Searchability by default may be in their short-term financial interest, but the end result can too easily be unusable security plus unsafe defaults." Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd edition, Wiley (April 14, 2008), page 742.

[64] "The use of SSL increases computational cost of the transactions by a factor of 5-7." Krishna Kant et al, *Architectural Impact of Secure Socket Layer on Internet Servers*, In Proceedings of the 2000 IEEE international Conference on Computer Design: VLSI in Computers & Processors (September 17 - 20, 2000). ICCD. IEEE Computer Society, Washington, DC, 7. See also: Li Zhaoet al *Anatomy and Performance of SSL Processing*, In Proceedings of the IEEE international Symposium on Performance Analysis of Systems and Software*, 2005* (March 20 - 22, 2005). ISPASS. IEEE Computer Society, Washington, DC, 197-206.

In June 2009, 38 industry and academic experts from the fields of computer security, privacy and law wrote an open letter to Google's Chief Executive Officer to chastise the company for its poor HTTPS defaults.[65] The company soon responded, stating that it is investigating the performance issues associated with enabling HTTPS by default, and that "unless there are negative effects on the user experience or it's otherwise impractical, we intend to turn on HTTPS by default more broadly, hopefully for all Gmail users."[66] The company has not yet enabled HTTPS by default, nor made any more information public regarding its stated plans to do so.

Of course, Google is not alone in leaving its users vulnerable to data theft. Users of Facebook, MySpace, Yahoo and Microsoft are equally vulnerable to the same attacks. Google does at least offer HTTPS encryption to those users who know to turn it on, while the other companies leave their users completely vulnerable to hackers. This problem, it seems, is industry wide.

### C. Cloud providers do not have an incentive to protect users

Banks and online merchants are legally required to bear the financial burden of online fraud, with consumer liability typically capped at just $50.[67] This responsibility provides the banks and merchants with a strong incentive to encrypt their customers' data as it is transmitted over the Internet as doing so will significantly reduce the risk of fraud or data loss for which they must otherwise pay.[68]

Unfortunately, similar incentives do not exist for the cloud computing providers. Most of these services do not charge their customers anything for the services that they provide, and thus never knowingly handle sensitive financial information such as credit cards. While many customers might feel that the information which they have entrusted to

---

[65] "Google is putting millions of users at risk of fraud from hackers and needs to enable encryption by default on its most popular web apps, including Gmail and Google Docs, a gaggle of security researchers told the search giant Tuesday in an open letter." Ryan Singel, Encrypt the Cloud, Security Luminaries Tell Google – Update, WIRED NEWS – Threat Level, June 16, 2009, available at http://www.wired.com/threatlevel/2009/06/google_ssl/. See also: Jacob Appelbaum et al, *Re: Ensuring adequate security in Google's cloud based services*, Open Letter to Google CEO Eric Schmidt, June 16, 2009, *available at* http://www.cloudprivacy.net/letter/.

[66] We know HTTPS is a good experience for many power users who've already turned it on as their default setting. And in this case, the additional cost of offering HTTPS isn't holding us back. But we want to more completely understand the impact on people's experience, analyze the data, and make sure there are no negative effects. Ideally we'd like this to be on by default for all connections, and we're investigating the trade-offs, since there are some downsides to HTTPS — in some cases it makes certain actions slower …. We're planning a trial in which we'll move small samples of different types of Gmail users to HTTPS to see what their experience is, and whether it affects the performance of their email. Does it load fast enough? Is it responsive enough? Are there particular regions, or networks, or computer setups that do particularly poorly on HTTPS? …. Unless there are negative effects on the user experience or it's otherwise impractical, we intend to turn on HTTPS by default more broadly, hopefully for all Gmail users. We're also considering how to make this work best for other apps including Google Docs and Google Calendar (we offer free HTTPS for those apps as well)." Alma Whitten, *HTTPS security for web applications*, Post to Google Online Security Blog, June 16, 2009, *available at* http://googleonlinesecurity.blogspot.com/2009/06/https-security-for-web-applications.html

[67] http://www.fdic.gov/regulations/laws/rules/6500-1350.html and the Truth in Lending Act.

[68] In fact, the large data breaches seen in 2008 and 2009 were a direct result of merchants not using encryption in their back-end systems, based on the (false) assumption that hackers would not be able to see this data in transit. See for example, Mark Jewell, *Encryption Faulted in TJX Hacking*, Associated Press, September 25, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/09/25/AR2007092500836.html

Google and Yahoo is sensitive, this data often does not fall into one of the select categories for which legally required data security standards exist, such as for medical data, social security numbers, and financial information.

While most users' word processing documents or photo collections may not be that valuable to a fraudster, an email account can have considerable value – due to the fact that inboxes routinely contain passwords and account information for *other* websites. For example, many Web sites will resend a password to a user's email address in the event that the user forgets her password. Thus, a poorly secured email account can be leveraged to gain access to a victim's bank account, brokerage account or online health records.

### D. The cloud computing industry suffers from market failure

If cars did not come with locks, the market would soon provide an incentive for manufacturers to add them. Once vehicle owners came back from a night out on the town and discovered their cars missing, these theft victims would soon tell their friends, and make certain to demand locks from the dealer during their next purchase.

No such consumer-driven incentives for security exist in the cloud computing industry. Consider that if a consumer's car is stolen, they usually learn of the theft rather promptly, as the car will be missing when they next attempt to use it. The theft or unauthorized access to an online account is different, since both the thief and the legitimate owner can concurrently access the same cloud based resource. That is, the user can continue to create and edit documents, while the thief is able to read each new memo and spreadsheet as they are created. The online account, unlike the stolen car, is a non-rivalrous good[69] (at least until the attacker changes the password and locks the user out). As a result, users of most cloud based services are not able to discover that something bad has happened and thus demand a solution from the service provider.[70]

Furthermore, once consumers do find out that their accounts have been hacked into, they are often not able to identify the event that lead to the unauthorized access. While a shattered car window reveals the entry point the thief used to break into a vehicle in order to steal a stereo, there is no tell-tale evidence left behind when a hacker snoops on an insecure cloud session conducted over a public wireless network in a coffee shop or library.

Most users of cloud computing services are unaware of the following:

1. Their private information is insecurely transmitted over the network,
2. That widely available technologies exist to provide for that secure transmission,
3. That the cloud service providers have opted to not deploy such safeguards and
4. That off-the shelf tools exist which can be used by hackers to easily break into their private email accounts and other cloud services.

Due to the widespread (yet understandable) ignorance of most end-users, it is not terribly surprising that all of the major cloud computing providers opt to ignore the encryption issue. There simply isn't sufficient market demand for these firms to allocate the considerable financial and engineering resources required to deploy encryption by default for all of their products. In a highly competitive industry with razor thin per-customer profits, there is no incentive to needlessly dedicate computing resources to something for which most customers have not expressed a want.

---

[69] "Rival goods are goods whose consumption by one consumer prevents simultaneous consumption by other consumers." See: http://en.wikipedia.org/wiki/Rivalry_(economics)

[70] Some companies, such as AOL's Instant Messenger, and Google's Gmail are the exception to this. Both companies tell users when another computer is currently logged into their account. Most cloud based services do not offer such a feature.

Encryption can be thought of as a shrouded product attribute similar to the cost of printer ink refills, or hidden fees associated with "free checking" bank accounts.[71] Consumers rarely consider the full cost of these products, because they do not calculate in the added costs of these shrouded attributes. When most consumers evaluate a cloud computing service, they likely consider the usability, speed and perhaps weigh in social factors – such as the number of their friends who are currently using it. Consumers are unlikely to consider the encryption offered (or not) by the service, particularly since most are not even aware of the existence of encryption when it is offered.[72]

In their seminal work analyzing markets with shrouded attributes, Gabaix and Laibson reveal that these goods can lead to two forms of exploitation in the market: Optimizing firms exploit myopic consumers through marketing schemes that shroud high-priced add-ons. In turn, sophisticated consumers exploit these marketing schemes. Simply put, by hiding the true cost of a product, a firm can offer the good at a lower initial price, since it will be able to recoup any lost profit via after-market sales. Savvy consumers can take advantage of this if substitute add-on goods (such as generic printer ink refills) are available. The paradox that Gabaix and Laibson identify is that this leads to a situation in which manufacturers have no incentive to ditch the shrouded good model, offer fairly priced goods, and advertise the evils practiced by their competitors. This is because each consumer educated about the shrouded attributes, rather than flocking to fair vendors, will instead purchase cheap after-market substitutes, and continue to purchase the subsidized shrouded good.

With this economic theory in mind, consider the market for encrypted cloud based services. Google offers HTTPS encryption for its services, but does not turn it on by default. If Google opts to turn encryption on by default, its cost of offering the service to each customer will go up. Assuming that its profits do not, the company will either have to make do with less profit per customer, or more likely, reduce the cost of operating the service through other means. Faced with such a situation, Google might have to lower the amount of free disk space it provides to each customer or switch to a model in which encryption is only offered to paying customers.

Faced with choice between two cloud providers, one that encrypts all traffic but offers less storage, and a service which only offers encryption to users savvy enough to enable the option and more disk space, most savvy users would opt for the latter provider. In this situation, naïve users subsidize those more savvy, by enabling them to enjoy both encryption and large disk quotas.

Thus, when one provider offers this subsidized form of encryption, it creates a strong disincentive for other firms to go down the path of encryption by default. Such a firm will be unable to compete for naïve customers, since it will have lowered the amount of disk space and other features in order to pay for the encryption related costs. This firm will also be unable to attract the savvy customers, since these will flock to providers which offer both encryption as well as large amounts of disk space.[73]

---

[71] "[C]onsumers sometimes fail to anticipate contingencies. When consumers pick among a set of goods, some consumers do not take full account of *shrouded product attributes*, including maintenance costs, prices for necessary add-ons, or hidden fees …. Shrouded attributes may include surcharges, fees, penalties, accessories, options, or any other hidden feature of the ongoing relationship between a consumer and a firm." Xavier Gabaix and David Laibson, *Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets*, Quarterly Journal of Economics, 2006 121:2, 505-540, *available at* http://www.econ.yale.edu/~shiller/behmacro/2003-11/gabaix-laibson.pdf.

[72] See generally: Stuart E. Schechter et al, *The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies*, In Proceedings of the 2007 IEEE Symposium on Security and Privacy (May 20 - 23, 2007). SP. IEEE Computer Society, Washington, DC, 51-65, *available at* http://www.usablesecurity.org/emperor/emperor.pdf

[73] This theory at least explains why only Google offers encrypted mail, word processing and spreadsheets. As for why no social networks offer HTTPS, we are still scratching our heads.

## E. Providing incentives for network encryption

One solution to the problem of excessive prices for after-market print supplies is to require printer manufacturers to prominently advertise the price per page at the place of purchase, thus making it easy for consumers to easily compare prices. In such a market with posted prices, printer manufacturers which sell higher printers with reasonably priced ink can compete with those which make use of shrouded ink prices.

A similar fix can be applied to the market for cloud based services – by requiring vendors to clearly disclose the risks of using their services without encryption. If consumers actually realize the risks they face when using unencrypted cloud based services, it may create sufficient market demand to encourage firms to provide their customers with encrypted services. Such a disclosure requirement could take the form of a mandatory notice, placed on the login pages for each cloud based service which lack HTTPS encryption.[74] Examples of such a notice could include:

> WARNING: Email messages that you write can be read and intercepted by others when you connect to this service using a public network (such a wireless network at a coffee shop, public library or school). If you wish to protect yourself from this risk, click here for a secure version of this service.
>
> WARNING: The word processing documents that you create using this service can be read and modified by others when you connect to this site using a public network (such a wireless network at a coffee shop, public library or school). Widely available technologies exist that will protect you from these risks, but this service provider has opted to not offer such protective functionality.

Such text would need to be prominently displayed, and not hidden deep within a web site's terms of service. However, Google's much publicized resistance to being forced to add any text to its web site,[75] it is quite likely that the company would opt to bear the financial burden of enabling encryption by default, rather than clutter up its "beautiful clean home page."[76]

While such a desire to keep their home pages clutter free might not motivate other companies, the increase in consumer awareness of the risks made possible through such mandatory labeling, might provide enough of a push in market demand to nudge these firms into offering such product functionality.

An alternative approach, of course, would simply be for the government to regulate providers of cloud computing services, as it has already done in the banking and health industries. Banks are simply not permitted to make

---

[74] These kinds of mandatory disclosure are a form of compelled commercial speech, and as such will only pass First Amendment scrutiny if it can be demonstrated that they serve a compelling state interest. Such analysis is beyond the scope of this article. For more on this area of the law, See: Robert Post, *Transparent and Efficient Markets: Compelled Commercial Speech and Coerced Commercial Associations in United Foods, Zauderer, and Abood*. Valparaiso University Law Review, Vol. 40, p. 555, 2006, *available at* http://ssrn.com/abstract=900210.

[75] "Google believes so strongly that adding the phrase "privacy policy" to its famously Spartan home page would distract users that it has picked a fight with an advertising trade group over the issue … Larry Page, the company's co-founder, didn't want a privacy link `on that beautiful clean home page,' … 'His argument is when you come to Google and you are looking for information, it is that big fat box' for search and little else, the executive said." Saul Hansell, *Google Fights for the Right to Hide Its Privacy Policy*, THE NEW YORK TIMES – Bits Blog, May 27, 2008, *available at* http://bits.blogs.nytimes.com/2008/05/27/google-fights-for-the-right-to-hide-its-privacy-policy/

[76] See id.

encryption a “choice” to be left up to consumers, just as auto manufacturers are no longer permitted to make seat belts an optional add-on for safety conscious car buyers.

We would prefer that regulators first force cloud computing providers to display clear educational warnings before those regulators go down the path of mandating specific technologies. However, if educational warnings fail to provoke a sufficient market response, stronger regulation might be appropriate.

## III. Personal privacy, cloud computing and the government

The preceding section focused on threats to user privacy from private actors, mainly hackers and other evil-doers who are able to easily hijack and steal cloud based user data. Such hacking happens without the direct knowledge or consent of the service provider, who will shut down such unauthorized access as soon as they learn about it.

This article will now shift focus to another serious threat to end-user privacy – one without easy fixes. The focus of this will be on invasions of user privacy in which the service provider is not only aware, but assists in the act, albeit due to coercion. In such cases, the surveillance occurs pursuant to a lawful order obtained by government agents,[77] and so even if the service provider wishes to protect its customers, it cannot.

The second part of this article will be arranged as follows: It will first explore the changing market dynamics which have made large-scale surveillance of electronic communications both easy and cheap for the government. As a result, the marginal cost of watching one more person has now dropped to essentially nothing. It will then briefly explore the third party doctrine, which is the primary legal doctrine which the Government relies on to force the disclosure of user information held by third parties, neutralizing the traditional Fourth Amendment protection offered to people’s personal documents and papers.

The solution to the privacy problems posed by the third party doctrine is actually rather simple – the mass deployment of encryption by software manufacturers and service providers. However, encryption alone is not the answer. This is due to government’s lawful powers of coercion, through which it can compel service providers to insert back doors in to their own products, circumventing the encryption that would otherwise protect their customers’ data. The core of this article will focus on this issue, and the way that this power to force the insertion of back doors can be applied to the providers of cloud computing services.

### A. The changing economics of surveillance

The mass adoption of digital technologies over the past decade has lead to a radical shift in the government's ability to engage in large scale surveillance.

Fifty years ago, if a government agency wished to monitor a suspect, it had to dedicate a number of agents to engage in around the clock physical surveillance and ask the post office to intercept and divert her mail, which would be steamed open, itself a labor intensive task. If phone surveillance was required, someone had to climb up a telephone pole or open an access panel attached to an apartment building in order to physically attach wires to the suspect’s line. With the tap in place, agents would need to monitor the calls around the clock. Finally, if investigators wished to

[77] In some cases, this may take the form of a warrant, but it may also be via a subpoena, or some other method in which there is little to no judicial oversight.

learn the contents of conversations spoken inside the home, a hugely laborious and risky "black bag job" would be necessary, in which highly skilled agents would break into the suspect's residence or workplace to covertly install microphones and remote transmitters.[78]

Times have changed, as have wiretapping techniques.[79] Telecommunications companies and Internet Service Providers now have dedicated legal compliance departments,[80] some open 24 hours per day, through which law enforcement agents can obtain wiretaps, emails, text messages or real time phone location information. Once contacted, service providers can usually process the request and initiate a wiretap with a few keystrokes – all without the need to enter the suspect's home or even manually connect wires in a switching center.[81]

Once the wiretap has begun, the customer's data is directly transmitted to the government servers.[82] While this transmission of a suspect's communications is typically performed on a case-by-case basis in response to specific requests, it appears that at least one telecommunications company has given the FBI wholesale access to its entire network, enabling agents to tap customers at will without requiring that the company's staff enable or assist with the

---

[78] "Since 1948 the FBI has conducted hundreds of warrantless surreptitious entries to gather domestic and foreign intelligence, despite the questionable legality of the technique and its deep intrusion into the privacy of targeted individuals. Before 1966, the FBI conducted over two hundred `black bag jobs.' These warrantless surreptitious entries were carried out for intelligence purposes other than microphone installation, such as physical search and photographing or seizing documents. Since 1960, more than five hundred warrantless surreptitious microphone installations against intelligence and internal security targets have been conducted by the FBI, a technique which the Justice Department still permits. Almost as many surreptitious entries were conducted in the same period against targets of criminal investigations … Surreptitious entries were performed by teams of FBI agents with special training in subjects such as `lock studies.'" Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Final Report: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Book III, S. Rep. No. 94-755, at 355 (1976)], *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIf.htm

[79] "We all know the scene: It is the basement of an apartment building and the lights are dim. The man is wearing a trench coat and a fedora pulled down low to hide his face. Between the hat and the coat we see headphones, and he appears to be listening intently to the output of a set of alligator clips attached to a phone line. He is a detective eavesdropping on a suspect's phone calls. This is wiretapping—as it was in the film noir era of 1930s Hollywood. It doesn't have much to do with modern electronic eavesdropping, which is about bits, packets, switches, and routers." Whitfield Diffie and Susan Landau, Communications Surveillance: Privacy and Security at Risk, ACM Queue, September 11, 2009, available at http://queue.acm.org/detail.cfm?id=1613130

[80] See generally: a list of the legal compliance departments at hundreds of phone/Internet companies: "ISP List", http://www.search.org/programs/hightech/isp/.

[81] "[S]ome 80 to 90 percent of old-fashioned wireline phone switches are apparently not CALEA compliant, which means the feds still have to perform those taps the old fashioned way. But every wireless switch in the country is CALEA read …. [and] over 80 percent of intercepts are now targeting wireless phones." *DCS-3000 is the FBI's new Carnivore*, Wired News – Threat Level, April 27, 2006, *available at* http://www.wired.com/threatlevel/2006/04/dcs3000_is_the_/

[82] "Aiding the easy listening is a 'dial-back' hack, in which phone company computers call up the law enforcement agency and pipe the customer's conversations down the open line." *DCS-3000 is the FBI's new Carnivore*, Wired News – Threat Level, April 27, 2006, *available at* http://www.wired.com/threatlevel/2006/04/dcs3000_is_the_/

surveillance.[83] Similarly, multiple Internet service providers have been accused of providing raw access to their "backbone" networks to the National Security Agency, which is then free to target individual communications for surveillance without the need to involve the communications companies.[84]

Even just 5 years ago, if the government wanted to get access to potentially incriminating evidence from the home computers of ten different suspects, investigators had to convince a judge that they had probable cause in order to obtain a search warrant for each person. The investigating agency would then send agents to raid the homes of the individuals, remove the computers, and later perform labor-intensive forensic analysis in order to get the files. In the event that the suspects knew each other, the government might opt to perform a simultaneous raid (thus requiring even more manpower), so that one suspect could not notify the others – who might then delete their files.

Now that many users have switched to cloud based services, digital search and seizure has become far easier. Law enforcement agencies have essentially deputized the technology companies that provide applications to end users, and made these firms a key component of the surveillance infrastructure.[85] Thus, the private documents of ten individuals can now be obtained through a single subpoena to Google or Microsoft – whose engineers will then locate the files (stored on the company's servers) and provide them to the government.

The shift to cloud computing obviously brings many benefits to law enforcement: significantly reduced manpower requirements, no need to go before a judge or establish probable cause in order to obtain a warrant, as well as the complete elimination of physical risk to agents who might be shot or attacked during a raid.

---

[83] "Because the data center was a clearing house for all Verizon Wireless calls, the transmission line provided the Quantico recipient direct access to all content and all information concerning the origin and termination of telephone calls placed on the Verizon Wireless network as well as the actual content of calls." Kevin Poulsen, *Whistle-Blower: Feds Have a Backdoor Into Wireless Carrier — Congress Reacts*, WIRED NEWS – Threat Level, March 6, 2008, *available at* http://blog.wired.com/27bstroke6/2008/03/whistleblower-f.html.

[84] "The cases allege that the government, in coordination with AT&T, intercepts communications (like phone calls and emails), and that AT&T illegally discloses communications records to the government. The core component of the surveillance is the government's nationwide network of sophisticated communications surveillance equipment, attached to the key facilities of telecommunications companies such as AT&T that carry Americans' internet and telephone communications. Through this shadow network of surveillance devices, the government has acquired and continue to acquire the content of the phone calls, emails, instant messages, text messages and web communications, both international and domestic, of practically every American who uses the phone system or the internet in an unprecedented suspicionless general search through the nation's communications networks." *NSA Spying FAQ*, Electronic Frontier Foundation, *available at* http://www.eff.org/nsa/faq

[85] "[Service providers] have, last time I looked, no line entry in any government directory; they are not an agent of any law enforcement agency; they do not work for or report to the Federal Bureau of Investigation ('FBI'); and yet, you would never know that by the way law enforcement orders them around and expects blind obedience." Albert Gidari Jr., Keynote Address: Companies Caught in the Middle, 41 U.S.F. L. Rev. 535, Spring 2007.

## B. Surveillance at near zero marginal cost

Modern surveillance technology is notable for the fact that the vast majority of the cost of systems is for up-front infrastructure. Intelligence and law enforcement agencies must purchase data centers filled with expensive computer equipment, and then develop custom software for initiating, recording, cataloging and indexing the wiretaps. The government has required that telecommunication companies upgrade to modern digital switches with digital intercept capabilities and provided hundreds of millions of dollars to help pay for this.[86]

Once these up front or predictable fixed costs (such as salaries for agents and lawyers) have been paid for, modern surveillance is surprisingly cheap, if it costs anything at all. In some cases, telecommunications companies and ISPs may charge to initiate and continue surveillance, as the law permits.[87] In other cases, the service providers may provide the information for free.

For those companies that do charge, surveillance can be a profit center.[88] A $50 per month home Internet connection can lead to hundreds of dollars in additional revenue when that customer is wiretapped,[89] while an $80 per month phone line can lead to thousands of dollars in revenue when it is wiretapped.[90] On the other hand, if a

---

[86] University of Pennsylvania professor Matt Blaze discovered that the Justice Department's Inspector General's office had failed to adequately obfuscate data in a March report … about FBI payments to telecoms to make their legacy phone switches comply with 1995 wiretapping rules. That report detailed how the FBI had finished spending its allotted $500 million to help telephone companies retrofit their old switches to make them compliant with the Communications Assistance to Law Enforcement Act … The FBI paid Verizon $2500 a piece to upgrade 1,140 old telephone switches. Oddly the report didn't redact the total amount paid to the telecom — slightly more than $2.9 million dollars." Ryan Singel, *Secret Data in FBI Wiretapping Audit Revealed With Ctrl+C,* WIRED NEWS – Threat Level, May 16, 2008, *available at* http://blog.wired.com/27bstroke6/2008/05/secret-data-in.html

[87] "Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance **shall be compensated therefor by the applicant for reasonable expenses** incurred in providing such facilities or assistance." 18 U.S.C. §§ 2518(4). "The Director of National Intelligence and Attorney General may direct a person to …. immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition … The Government **shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance** pursuant to subsection (e)." The Foreign Intelligence Surveillance Act, as amended by the 2008 Protect America Act.

[88] "In the end, it could be that the phone companies that cooperated with the NSA did so not for reasons of patriotism, or because their arms were twisted, but because the NSA came with a checkbook. Taking the NSA's money may be the only remaining profit center in bit-shipping. " Andrew Appel, *Eavesdropping as a Telecom Profit Center*, Post to Freedom To Tinker Blog, October 31, 2007, *available at* http://freedom-to-tinker.com/blog/appel/eavesdropping-telecom-profit-center

[89] "Upon lawful request and for a thousand dollars, Comcast, one of the nation's leading telecommunications companies, will intercept its customers' communications under the Foreign Intelligence Surveillance Act. The cost for performing any FISA surveillance 'requiring deployment of an intercept device' is $1,000.00 for the 'initial start-up fee (including the first month of intercept service),' according to a newly disclosed Comcast Handbook for Law Enforcement. Thereafter, the surveillance fee goes down to '$750.00 per month for each subsequent month in which the original [FISA] order or any extensions of the original order are active.'" Steven Aftergood, *Implementing Domestic Intelligence Surveillance*, Secrecy News, Federation of American Scientists, October 15, 2007, *available at* http://www.fas.org/blog/secrecy/2007/10/implementing_domestic_intellig.html.

[90] "Over 80 percent of intercepts are now targeting wireless phones, though the fancy CALEA taps can cost as much as $2,600 for 30 days of spying," *DCS-3000 is the FBI's new Carnivore*, Wired News – Threat Level, April 27, 2006, *available at* http://www.wired.com/threatlevel/2006/04/dcs3000_is_the_/ "To defer the cost to Cox of compliance, payment of the following minimum fees is required for all subpoena, court order and warrant requests …. Wiretap: **$2,500** for each 30 days —

telecommunications company provides the government unfettered access to its backbone network, wiretaps are essentially free – since the equipment, leased data lines and agent manpower would be paid for no matter how many individuals are being watched.

With the surveillance infrastructure in place, all that law enforcement agents need to do is to issue a couple commands from a computer terminal, at which point, a government server will begin capturing a suspect's raw telephone, Internet and other traffic. Automated software can scan the contents of the calls and emails, and a summary report can be sent to an agent if there are any matches. The interception itself requires little to no direct supervision, and so it is just as easy to tap 1, 50 or 100 additional suspects.

### C. The problem with free and cheap surveillance

Telecommunication companies often act as a form of oversight for surveillance requests – primarily due to their fear of being sued for assisting with illegal wiretapping. In several past instances, companies have refused to comply with surveillance orders that they believed were illegal.[91] Federal wiretapping laws outline specific civil liabilities for companies that provide customer information without meeting the appropriate legal requirements. This liability gives telecommunication companies a strong incentive to insist that the law is being followed. Thus, when wiretaps can be performed without any involvement of the telecommunication providers, consumers are robbed of this crucial additional layer of oversight, and must rely upon law enforcement and intelligence agencies to not abuse their access.

Another spillover benefit of the pay-for-surveillance model is that it creates a paper-trail.[92] That is, if the government is billed for each wiretap it requests, a billing record will be generated detailing the date that tap began, ended, the

---

**$2,000** for each additional 30 days." Notice to parties serving subpoenas on Cox Communications, March 01, 2008, *available at* http://www.cox.com/Policy/leainformation/default.asp.

[91] "In May 2006, USA Today reported that the NSA had been secretly collecting the phone-call records of tens of millions of Americans, using data provided by major telecom firms. Qwest, it reported, declined to participate because of fears that the program lacked legal standing …. '[Qwest's CEO] made inquiry as to whether a warrant or other legal process had been secured in support of that request …. When he learned that no such authority had been granted and that there was a disinclination on the part of the authorities to use any legal process, including the Special Court which had been established to handle such matters, [he] concluded that these requests violated the privacy requirements of the Telecommunications Act." Ellen Nakashima and Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, WASHINGTON POST, October 13, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485.html. "In a rare public ruling, a secret federal appeals court has said telecommunications companies must cooperate with the government to intercept international phone calls and e-mail of American citizens suspected of being spies or terrorists. The ruling came in a case involving an unidentified company's challenge to 2007 legislation that expanded the president's legal power to conduct wiretapping without warrants for intelligence purposes." James Risen and Eric Lichtblau, *Court Affirms Wiretapping Without Warrants*, THE NEW YORK TIMES, January 15, 2009, *available at* http://www.nytimes.com/2009/01/16/washington/16fisa.html.

[92] "Compensation generally equals sunshine and transparency. Currently, if service providers are not paid to implement wiretap solutions, if they are not paid to produce thousands and thousands of records, there is no audit trail. And if there is no audit trail, there is no visibility and transparency into how the money is spent, and you do not know what capabilities are actually being acquired …. When I can follow the money, I know how much of something is being consumed - how many wiretaps, how many pen registers, how many customer records. Couple that with reporting, and at least you have the opportunity to look at and know about what is going on. Because right now, you do not know." Albert Gidari Jr., Keynote Address: Companies Caught in the Middle, 41 U.S.F. L. Rev. 535, Spring 2007.

number or customer tapped, as well as the cost of this service. At least two copies of this will be generated, one for the ISP and another sent to the investigating agency. This paper trail provides a wealth of data for oversight bodies, and the fear of creating such a paper trail may dissuade investigators from initiating surveillance without the appropriate evidence.

Finally, per-transaction-billing based surveillance brings the benefit of scarcity. That is, given a fixed size budget, and a practically endless number of possible suspects, government agents are forced to prioritize their surveillance efforts. This provides a strong incentive for them to focus on investigations likely to bear fruit, as well as to stay away from "fishing expeditions."

Even in the event that a provider charges for surveillance assistance, this situation is still much better for government agents than in the pre-digital days. Sending agents out to monitor a home or trail a suspect consumes significantly more resources than paying an ISP $1000 to turn on a wiretap or locate a mobile phone. It is also much safer.

Obtaining and serving a warrant upon a suspect, raiding her home, and seizing her computers not only consumes valuable agent hours,[93] but it places agents in harm's way. A suspect could be armed, or have protected his home with booby traps. While law enforcement agencies might mitigate this risk through the use of SWAT style tactics,[94] the risk to their own is still there. This risk of physical harm provides an additional and highly personal incentive for officers to limit such searches. However, now that cloud computing companies are able to provide law enforcement with the documents that would have once required an armed raid, this risk of physical harm is gone, and with it, whatever disincentives for over-reach it provided.

### D. Cloud providers and the third-party doctrine

The Fourth Amendment guarantees all Americans a measure of control around their bodies and possessions that the government cannot enter or search without reasonable cause. Thus, a person's diary, personal letters, and other such property are normally provided with constitutional protection. Americans have become used to these rights, and often take for granted that private matters are usually kept private. Unfortunately, as society has shifted to communicating and working online, these constitutional protections have been left behind.

Fourth Amendment protections against unreasonable search and seizure depend upon a person's reasonable expectation of privacy. Unfortunately for users of Internet based services, existing case law does little to protect their digital documents and papers which are now increasingly being stored on the remote servers of third parties.

The cause of this departure from the Fourth Amendment: the third party doctrine, which establishes that people have no expectation of privacy in the documents they share with others. Rather than revisit *Smith v. Maryland* and *United States v. Miller* at length, a single quote from the Supreme Court should be enough:

---

[93] "Warrants are costly to the police: they require both paperwork and hours hanging around a courthouse waiting to see the magistrate … Both the warrant and probable cause requirements, then, make house searches considerably more expensive for police than those searches would be absent those requirements. The rules function as a tax, payable in police time rather than money. When a police officer decides to search a house or apartment, he must first spend several hours performing tasks that the law says are prerequisites to such a search … if you tax a given kind of behavior, you will probably see less of it." William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 Geo. Wash. L. Rev. 1265 (1998-1999).

[94] See generally, Radley Balko, *Overkill: The Rise of Paramilitary Police Raids in America*, white paper, The Cato Institute, July 17, 2006, *available at* http://www.cato.org/pubs/wtpapers/balko_whitepaper_2006.pdf

> "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed to him by Government authorizes, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[95]

The third party doctrine is the "Fourth Amendment rule that scholars love to hate," "widely criticized as profoundly misguided", and decisions applying the doctrine "top[] the chart of [the] most criticized Fourth Amendment cases."[96] However, for the purposes of this article, it can be summarized by stating that online service providers can be compelled to reveal their customers' private documents with a mere subpoena.[97] As such, the government is not required to obtain a search warrant,[98] demonstrate probable cause[99] or go before a judge.

While the third party doctrine is certainly the current tool of choice for the government's evisceration of the Fourth Amendment, is not completely to blame for the lack of privacy online. The real and often overlooked threat to end-user privacy is not this legal rule, but the industry-wide practice of storing customers' data in plain text, forgoing any form of encryption. Simply put, if encryption were used to protect users' stored data, the third party doctrine would for the most part be moot.

Thus, this article must now analyze the failure of the market to provide end-users with this crucial protection from warrantless government intrusion.

### E. Why we don't have widespread encrypted cloud services

First, a few definitions for different kinds of encryption: Network encryption (typically HTTPS) is used to protect data as it is transmitted from the client to a server. Data encryption is used to protect the data once it is in storage. Within this latter category, there are two particular styles of use: data encryption in which the service provider knows the encryption key, and data encryption in which the service provider does not know the encryption key.

Network encryption only protects data in transit, and so the use of this technology does nothing to protect users' data from a subpoena. Likewise, if a cloud provider has both the user's data, and the key used to encrypt it, the

---

[95] United States v. Miller, 307 U.S. 174 (1939).

[96] Orin S. Kerr, *The Case for the Third-Party Doctrine*, Michigan Law Review, Vol. 107, 2009, *available at* http://ssrn.com/abstract=1138128

[97] See, for example, **Gonzales v**. **Google Inc**., 234 F.R.D. 674 (N.D. Cal. 2006).

[98] "Because ISPs are third parties, and usually corporate entities at that, the government will not ordinarily search the servers of ISPs directly. The government will instead seek a court order compelling the network provider to disclose the information to the government. This is important because the Fourth Amendment generally allows the government to issue a grand jury subpoena compelling the disclosure of information and property, even if it is protected by a Fourth Amendment `reasonable expectation of privacy.'" Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, George Washington Law Review, 2004, at page 5, *available at* http://ssrn.com/abstract=421860

[99] "When the government obtains a court order such as a subpoena that requires the recipient of the order to turn over evidence to the government within a specified period of time, the order will generally comply with the Fourth Amendment if seeks relevant information and is not overbroad. No probable cause is required." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, George Washington Law Review, 2004, at page 5, *available at* http://ssrn.com/abstract=421860

company can be compelled to produce both. The only real protection from government intrusion comes with the encryption of data with a key that only the user knows.

As this article will now argue, there are two main reasons why most cloud providers have not gone down this path.

### *1. A lack of perceived consumer demand for encryption of stored data*

As explained earlier, network encryption can protect data from passive adversaries who try to capture data as it is transmitted from the customer's computer to the cloud provider. Encryption of the data in storage protects against a different set of threats. If the service provider knows the encryption key, the user still gains significant protection from data loss risks – that is, misplaced backup tapes and stolen laptops, providing the company is not storing the encryption key on the same media as the encrypted user data.

Data encryption with a key that is private to the user protects against a very specific set of threats – including so called insider attacks, where an employee "peeps" at customer data,[100] and legally compelled disclosure. These are two potential risk scenarios which companies have little to no incentive to publicize. Simply put, service providers likely prefer that their customers not know these risks exist.

While it is little known to most consumers, government requests to Web 2.0 companies have become a routine part of business.[101] Practically all cloud computing providers have dedicated legal compliance departments,[102] some open 24 hours per day, through which law enforcement agents can obtain emails, logs of search requests and other stored customer data through a formalized process[103]. While Google has widely publicized its initial refusal to deliver search records in response to a request by the US Department of Justice in 2006, it has been far less willing to discuss the huge number of subpoenas it receives per year, to which it does comply and thus deliver its customers' data to law

---

[100] See generally, Peter P. Swire, *Peeping*, Berkley Technology Law Journal, Forthcoming 2009, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1418091. Facebook serves as a classic example of this privacy threat: "Valleywag kept hearing reports that Facebook employees had violated their users' privacy in a number of ways. The claimed abuses varied: Looking at restricted profiles to check out dates. Seeing which profiles a user had viewed. And, in one case, allegedly logging onto a user's account, changing her profile picture to a graphic image, and sending faked messages …. Facebook may have sophisticated privacy controls. But they don't appear to be deployed at headquarters." Owen Thomas, *Why Facebook employees are profiling users*, VALLEYWAG, October 29, 2007, *available at* http://valleywag.gawker.com/316469/why-facebook-employees-are-profiling-users.

[101] "Who is sending threatening e-mail to a teenager? Who is saying disparaging things about a company on an Internet message board? Who is communicating online with a suspected drug dealer? These questions, and many more like them, are asked every day of the companies that provide Internet service and run Web sites. And even though these companies promise to protect the privacy of their users, they routinely hand over the most intimate information in response to legal demands from criminal investigators and lawyers fighting civil cases." Saul Hansel, *Increasingly, Internet's Data Trail Leads To Court*, NEW YORK TIMES, February 4, 2006, *available at* http://www.nytimes.com/2006/02/04/technology/04privacy.html.

[102] See generally a list of the legal compliance departments at hundreds of phone/Internet companies: "ISP List", http://www.search.org/programs/hightech/isp/.

[103] "Requests for information have become so common that most big Internet companies, as well as telephone companies, have a formal process for what is often called subpoena management. Most of the information sought about users is basic, but very personal: their names, where they live, when they were last online — and, if a court issues a search warrant, what they are writing and reading in their e-mail." Saul Hansel, *Increasingly, Internet's Data Trail Leads To Court*, NEW YORK TIMES, February 4, 2006, *available at* http://www.nytimes.com/2006/02/04/technology/04privacy.html.

enforcement agencies.[104] Furthermore, the company's CEO has publicly stated that one of the main reasons the company retains detailed data on consumers' online activity is to assist the government with lawful investigations.[105] However, Google is not alone in not wishing to discuss the frequency of government requests – there seems to be an industry-wide policy of silence.[106] Only Facebook and AOL have broken the silence to disclose even approximate numbers – 10-20 per day and 1000 requests per month respectively.[107] Of course, these numbers only reveal a portion of the government's quiet collection of private data – as requests made in response to FBI National Security Letters and FISA court orders are typically gagged, and thus never disclosed, even in aggregate form.

It would be wrong to assume that consumers do not care the ease with which their private information can be disclosed. For example, in early 2009, Sweden passed a new law requiring Internet Service Providers to hand over customer's information to intellectual property holders investigating piracy. Swedish Internet traffic dropped by over 30 percent starting the day that the new law came into effect.[108] This clear demonstration of consumer's privacy fears then lead to competition in the market for privacy-preserving services. Within weeks, three of Sweden's Internet Service Providers had announced new policies in which they would not retain any information linking IP address

---

[104] "The new policy also shouldn't affect many investigations, [Google Deputy Counsel Nicole] Wong said, since the two year time limit 'seems to be at the outer edge of what police want.' Mostly police are interested in logs that are a day or two old, according to Wong. Google still refuses to disclose how often their logs are subpoenaed, even in cases where they are free to do so." Ryan Singel, *Google To Anonymize Data — Updated*, WIRED NEWS – Threat Level, March 14, 2007, *available at* http://www.wired.com/threatlevel/2007/03/google_to_anony/. "As a matter of policy, we do not comment on the nature or substance of law enforcement requests to Google." Declan McCullagh, *How safe is instant messaging? A security and privacy survey*, CNET NEWS, June 9, 2008, *available at* http://news.cnet.com/8301-13578_3-9962106-38.html.

[105] "The reason we keep [search engine data] for any length of time is one, we actually need it to make our algorithms better, but more importantly, there is a legitimate case of the government, or particularly the police function or so forth, wanting, with a federal subpoena and so forth being able to get access to that information." Eric Schmidt, All Things Considered, NATIONAL PUBLIC RADIO, between 5:40 and 6:40, October 2, 2009, *available at* http://www.npr.org/templates/story/story.php?storyId=113450803

[106] "We do not comment on specific requests from the government. Microsoft is committed to protecting the privacy of our customers and complies with all applicable privacy laws. In particular, the Electronic Communications Privacy Act ("ECPA") protects customer records and the communications of customers of online services. As set forth above, however, Microsoft does not maintain records about our customers' use of the IM service and would have no information to provide in response to a request from law enforcement." and "Given the sensitive nature of this area and the potential negative impact on the investigative capabilities of public safety agencies, Yahoo does not discuss the details of law enforcement compliance. Yahoo responds to law enforcement in compliance with all applicable laws." Declan McCullagh, *How safe is instant messaging? A security and privacy survey*, CNET NEWS, June 9, 2008, *available at* http://news.cnet.com/8301-13578_3-9962106-38.html.

[107] "[Facebook] says it tends to cooperate fully and, for the most part, users aren't aware of the 10 to 20 police requests the site gets each day." Nick Summers, *Walking the Cyberbeat*, NEWSWEEK, May 1, 2009, *available at* http://www.newsweek.com/id/195621. "AOL, for example, has more than a dozen people, including several former prosecutors, handling the nearly 1,000 requests it receives each month for information in criminal and civil cases…. AOL says that only 30 of the 1,000 monthly requests it receives are for civil cases, and that it initially rejects about 90 percent of those, arguing that they are overly broad or that the litigants lack proper jurisdiction. About half of those rejected are resubmitted, on narrower grounds." Saul Hansel, *Increasingly, Internet's Data Trail Leads To Court*, NEW YORK TIMES, February 4, 2006, *available at* http://www.nytimes.com/2006/02/04/technology/04privacy.html.

[108] The new law, which is based on the European Union's Intellectual Property Rights Enforcement Directive (IPRED), allows copyright holders to obtain a court order forcing ISPs to provide the IP addresses identifying which computers have been sharing copyrighted material … traffic fell from an average of 120Gbps to 80Gbps on the day the new law came into effect." *Piracy law cuts internet traffic*, BBC NEWS, April 2, 2009, *available at* http://news.bbc.co.uk/2/hi/technology/7978853.stm

information to particular customers. Explaining the motivation for change in policy, the CEO of one of the country's largest ISPs said that "it's a strong wish from our customers, so we decided not to store information on customers' IP numbers."[109]

There is one significant difference between most cloud computing providers and the Swedish ISPs who responded to the market demand for privacy: Money. The Swedish ISPs' primary source of revenue is the monthly fees which they charge their customers for broadband Internet services. However, the cloud computing providers generally provide their services for free, and make their money by collecting large amounts of consumer data, which they then monetize through the sale of highly targeted advertising. While the ISPs can easily afford to do without detailed consumer data, the cloud computing providers cannot, at least as their business models currently stand. Their profit margins depend upon their ability to convince customers to trust them with *more* private data, not less.

### *2. Business models that depend on advertising and data mining*

It is exceedingly difficult to monetize a data set that you cannot look at. Google's popular Gmail service scans the text of individual emails, and algorithmically displays relevant advertisements next to the email. When a user receives an email from a friend relating to vacation plans, Google can display an advertisement for hotels near to the destination, rental cars or travel insurance. If those emails are encrypted with a key not known to Google, the company is unable to scan the contents and display related advertising. Sure, the company can display generic advertisements unrelated to the user's communications contents, but these will be far less profitable.[110]

Google's Docs service, Microsoft's Hotmail, Adobe's Photoshop Express, Facebook, and MySpace are all made available for free. Google provides its users with gigabytes of storage space, yet doesn't charge a penny for the service. These companies are not charities, and the data centers filled with millions of servers required to provide these services cost real money. The companies must be able to pay for their development and operating costs, and then return a profit to their shareholders. Rather than charge their users a fee, the firms have opted to monetize their user's private data. As a result, any move to protect this data will directly impact the companies' ability to monetize it and thus turn a profit.[111] Barring some revolutionary developments from the cryptographic research community, advertising based business models are fundamentally incompatible with private key encrypted online data storage services.

Advertising is not the only way to pay for cloud computing. Over the past few, Google has convinced 500,000 businesses and organizations to switch to its "Apps for Domains" product, in which it provides Mail, Docs, Spreadsheets and other cloud based services to companies, universities, and governments. Google does not mine

---

[109] Mats Lewan, *Swedish ISPs vow to erase users' traffic data*, CNET NEWS, April 28, 2009, *available at* http://news.cnet.com/8301-1023_3-10229618-93.html.

[110] "Click-Through Rate (CTR) of an ad can be averagely improved as high as 670% by properly segmenting users for behavioral targeted advertising." Jun Yan et al, *How much can Behavioral Targeting Help Online Advertising?*, In Proceedings of the 18th international Conference on World Wide Web (Madrid, Spain, April 20 - 24, 2009). WWW '09. ACM, New York, NY, 261-270, *available at* http://www2009.eprints.org/27/1/p261.pdf

[111] "If Google can build a higher–quality data set of customer information, they can charge more per advertisement, whilst also gaining a significant market advantage over the other search engines." Christopher Soghoian, *The problem of anonymous vanity searches*, I/S: A Journal of Law and Policy for the Information Society, Volume 3, Issue 2, 2007, *available at* http://ssrn.com/abstract=953673.

these corporate customers' email for advertising purposes, and instead charges $50 per user per year, which is more than enough to pay the costs of operating the service and make a profit. Likewise, Microsoft offers its Office Live based suite to corporate customers wishing to pay a per user fee. If customers, particularly those in the corporate and government space were willing to pay for the higher development and computational costs required for encryption, it is quite likely that companies like Google and Microsoft might compete to meet the market demand.

### F. Encryption in the cloud

Cloud based services do not, by their very nature, have to put the privacy of their users at risk. Consider, as an example, the Weave software add-on for the Firefox web browser.[112] This tool enable users to keep their bookmarks, browsing history, saved passwords, and cookies synchronized across multiple computers. The tool even supports the Firefox mobile phone browser, allowing users to bookmark a web page at home and then later view it while commuting to work from their phone.

Like all cloud services, The Mozilla Corporation (which makes Firefox and Weave) is able to provide this instant, worldwide access by allowing users to store their own data on Mozilla's servers. However, Mozilla baked privacy into the product at the design stages, stating that a key principle of the project that "users own their data, and have complete control over its use. Users need to explicitly enable third parties to access their data."[113] As a result, the data that Weave users store on Mozilla's servers is encrypted with a key created by that user, which is not shared with anyone else. Mozilla simply provides the cloud-based storage, but is unable to peek at its users' stored passwords and browsing history. In the event that law enforcement or intelligence agencies seek to compel Mozilla to share its users' data, the company can confidently hand over the encrypted files with the knowledge that the data is complete gibberish to everyone but its owner.

Mozilla has not attempted to monetize the Weave service, which is perhaps why it has been able to put user privacy first. It has even provided an open source Weave server, so that other groups and companies can provide their own cloud-based storage for Weave users.

Building on Weave, imagine a situation in which Google, Microsoft and the other providers follow Mozilla's example, and build strong encryption into their own services, such that only users will have the ability to decrypt their own data.

In this hypothetical scenario, Google's Docs word processor will store each user's files in an encrypted form on Google's vast array of servers. When the user loads the Google Docs application in their Web browser, it will prompt the user for her password. The Web application will then request copies of the most recent documents from Google's servers, download them, and then decrypt these files locally in the browser. As the user makes changes to the documents, the modifications will be encrypted, and then transmitted to Google's servers. Users will still be able to access their own documents from any computer around the world, yet the documents will be safe from the prying eyes of governments, divorce lawyers, and even inquisitive rogue Google employees.

Such a scenario is not beyond the realm of imagination. Certainly, as Mozilla's Weave has demonstrated, it is technically possible to build privacy into the cloud. Were the cloud computing industry to follow Mozilla's example

---

[112] *Introducing Weave*, Mozilla, Dec. 12, 2007, *available at* http://labs.mozilla.com/2007/12/introducing-weave

[113] Overview of OAuth for Weave, https://wiki.mozilla.org/Labs/Weave/OAuth

and encrypt all user data, the warrant-free access of individual's private data made possible by the third party doctrine would become a thing of the past.

### G. How encryption will change the status quo

A move to encrypted cloud based services will likely lead to a significant reduction in the ease with which law enforcement agents can obtain the private files of suspects. I consider this to be a feature, not a bug. Simply put, cloud computing and the online storage of data by third parties has made law enforcement far too cheap. It is time for a market adjustment.

Nevertheless, the law enforcement and intelligence communities will likely argue that without the ability to force service providers to reveal their customer's communications, government agents will be unable to catch pedophiles and terrorists.[114]

While I certainly wish to roll back the effectiveness, scale and extreme low cost at which the government can currently engage in surveillance, I also recognize that there is a legitimate need to investigate suspects. Luckily, even with the widespread use of encryption, there is still a way for government agents to get access to data: the black bag job, a search method already in widespread use.[115]

As noted earlier in this article, in the days before easy wiretaps at the phone company, law enforcement agencies had to send an agent out to tap the line at the suspect's home, or perhaps scale a nearby telephone pole. The widespread use of encryption brings us back to a form of surveillance dependent upon manual labor. The *Scarfo* case provides a fantastic example of this, in which a suspect's use of disk encryption was defeated by the FBI. A team of agents snuck into Scarfo's home, planted microphones and other recording devices in his computer, which then captured a copy of his password as he typed it on the keyboard.[116] No matter how strong the encryption, the human is always the weakest link, and the black bag job exploits this.

---

[114] "I doubt that Congress would pass on the opportunity to make sure that our children were safe from terrorists." Quoting FBI director Louis Freeh speaking before a House of Representatives hearing on the FBI's Digital Telephony bill, 09/13/94 Electronic Frontier Foundation, EFF Quotes Collection 19.6 (Apr 9, 2001), available at http://w2.eff.org/Misc/EFF/?f=quotes.eff.txt. "In a private meeting with industry representatives, [Attorney General] Gonzales, [FBI Director] Mueller and other senior members of the Justice Department said Internet service providers should retain subscriber information and network data for two years … During Friday's meeting, Justice Department officials passed around pixellated (that is, slightly obscured) photographs of child pornography to emphasize the lurid nature of the crimes police are trying to prevent." Declan McCullagh, Gonzales pressures ISPs on data retention, CNET NEWS, May 26, 2006, *available at* http://news.cnet.com/2100-1028_3-6077654.html

[115] "A total of 763 [delayed notice search] warrant requests and 528 requests for [delayed notice] extensions were reported for the fiscal year ended September 30,2008 …. Drug offenses were specified in 65 percent of applications reported, followed by fraud (5 percent), weapons, and tax offenses (4 percent each)." Report the Director of the Administrative Office of the United States Courts on Applications for Delayed-Notice Search Warrants and Extensions, July 2, 2009, *available at* http://big.assets.huffingtonpost.com/SneakAndPeakReport.pdf. This number does not include most covert searches conducted as part of terrorism and intelligence investigations, as "surveillance methods are 'generally covert altogether,' and do not use sneak-and-peek warrants." See: http://rawstory.com/blog/2009/09/patriot-act-regular-crimes/ (describing testimony of Assistant Attorney General David Kris before the Senate Judiciary Committee on September 23, 2009).

[116] *United States v Scarfo*, 180 F Supp 2d 572 (D NJ 2001) (describing investigation using key logger to intercept passwords).

What this article proposes is not the end to the lawful acquisition of investigative data, merely that law enforcement no longer be able to deputize service providers into quietly disclosing their customer's data. If a suspect is important enough, let the police dedicate the significant manpower to break into her home in order to install bugs. Given the finite limit to the financial and human resources available to law enforcement agencies, such a change in the balance of power, by raising the effective cost of such surveillance, would force investigators to prioritize their targets, and shy away from fishing expeditions.[117]

Furthermore, such a dependence on black bag jobs would also bring a further (and significant) benefit long sought by privacy activists: The return of the Fourth Amendment. If police need to break into a suspect's home in order to try and install a password-stealing bug, they must first obtain a search warrant, and thus find themselves firmly back in the familiar domain of the Fourth Amendment. This would lead to at least some judicial oversight of investigations, something that is almost entirely absent under the current subpoena standard.

As much as a move to widespread encryption would cheer up privacy activists, encryption technology is not a magic bullet. As this article will now explain, even if cloud computing providers deploy encryption technology, the government retains an extremely powerful trump card: the ability to force service providers to insert covert back doors into their own products.

## IV. Companies can be forced to turn against their customers

When consumers purchase technology, it is typically because they want to perform some task or function. It is exceedingly unlikely that purchases are made with the goal of making it easier for the government to spy on the purchaser. However, firms are now regularly compelled to modify their products in order to facilitate the government's interest in surveillance and search. Consumers are essentially subsidizing the government's intrusions into their own private records, and in the vast majority of cases, the consumer never knows it.

Consumers have significantly reduced privacy rights when they are spied upon with their own devices and software. For example, while government agents are required to first obtain a warrant in order to use a GPS tracking device that they have covertly placed on a person or their vehicle to track their moments on private property,[118] that same location information can be obtained from the suspect's cellular phone provider with a mere subpoena. Furthermore, even if a company attempts to build privacy-protections into its products, these can be quietly neutralized. Technology providers are frequently forced to circumvent the privacy protections they have built into their products and insert backdoors – adding new features, the sole purpose of which is to violate the privacy of the customer. We now present a few examples of this.

---

[117] "Where there are more crimes than the police can investigate, the police must, by definition, choose which crimes to investigate. Anything that makes investigating some crimes more expensive will tend to drive police toward other crimes, in the same way that making airplane travel more expensive will drive passengers to trains or cars … Some police tactics are wholly unregulated, some are regulated lightly, and a few, like house searches, are regulated fairly heavily. In a world like that, a world where the law taxes some kinds of policing more than others, the likely substitutions will occur within policing, not outside it, as the police shift time and energy away from more expensive (because more highly taxed) tactics and toward cheaper ones." William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 Geo. Wash. L. Rev. 1265 (1998-1999).

[118] 18 U.S.C. §§ 3117. See also: Jeff Wealty, *GPS Tracking Devices and the Fourth Amendment*, October 2008, *available at* http://www.sog.unc.edu/programs/crimlaw/GPS%20Tracking%20Devices%20and%20the%20Fourth%20Amendment.pdf

### A. The FBI's Magic Lantern / Computer and Internet Protocol Address Verifier (CIPAV)

In 2001, it was revealed that the FBI had developed a malicious software suite for the purpose of stealing information from suspects' computers.[119] The "Magic Lantern" tool (since renamed the Computer and Internet Protocol Address Verifier or CIPAV) has much in common with typical computer viruses – namely, the FBI relies upon un-patched vulnerabilities in a suspect's computer to gain unauthorized access and then covertly installs their data evidence gathering software. However, rather than sending a victim's private documents back to an identify thief in Eastern Europe, the personal files are instead sent to a FBI computer in Quantico, Virginia.[120]

All available information on the use of CIPAV seems to indicate that the tool is only used after law enforcement officers have obtained a search warrant. However, the revelation of the tool's existence did lead to a media firestorm when Network Associates reportedly told the Associated Press that the company would be willing to modify its popular McAfee Anti-Virus software suite to ignore the FBI's spyware tool.[121] That is, customers who purchased the anti-virus suite would not be warned if their computers were infected by an FBI-written virus.

In a 2007 survey of 13 anti-spyware vendors, all of the companies stated that their policy was to detect all forms of spyware, including software made by the government.[122] However, when asked if they had ever received a court order requiring the white-listing of government spyware, both Microsoft and Network Associates declined to comment.[123]

---

[119] Nat Hentoff, *The FBI's Magic Lantern*, THE VILLAGE VOICE, May 28th, 2002, *available at* http://www.villagevoice.com/2002-05-28/news/the-fbi-s-magic-lantern/1

[120] "The full capabilities of the FBI's "computer and internet protocol address verifier" are closely guarded secrets, but here's some of the data the malware collects from a computer immediately after infiltrating it, according to a bureau affidavit acquired by Wired News: IP address; MAC address of ethernet cards; A list of open TCP and UDP ports; A list of running programs; The operating system type; version and serial number; The default internet browser and version; The registered user of the operating system, and registered company name, if any; The current logged-in user name; The last visited URL …. All that information is sent over the internet to an FBI computer in Virginia, likely located at the FBI's technical laboratory in Quantico." Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED NEWS, July 18, 2007, *available at* http://www.wired.com/politics/law/news/2007/07/fbi_spyware.

[121] "Network Associates has been snared in a web of accusations over whether it will place backdoors for the U.S. government in its security software …. An Associated Press article then reported that 'at least one antivirus software company, McAfee Corp., contacted the FBI ... to ensure its software wouldn't inadvertently detect the bureau's snooping software and alert a criminal suspect.'" Declan McCullagh, *'Lantern' Backdoor Flap Rages*, WIRED NEWS, November 27, 2001, *available at* http://www.wired.com/politics/law/news/2001/11/48648.

[122] "Some companies that responded to the survey were vehemently pro-privacy. 'Our customers are paying us for a service, to protect them from all forms of malicious code,' said Marc Maiffret, eEye Digital Security's co-founder and chief technology officer. 'It is not up to us to do law enforcement's job for them so we do not, and will not, make any exceptions for law enforcement malware or other tools.' Declan McCullagh and Anne Broache, *Will security firms detect police spyware?*, CNET NEWS, July 17, 2007, *available at* http://news.cnet.com/Will-security-firms-detect-police-spyware/2100-7348_3-6197020.html.

[123] "'Microsoft frequently has confidential conversations with both customers and government agencies and does not comment on those conversations,' a company representative said. Of the 13 companies surveyed, McAfee was the other company that declined to answer … Cris Paden, Symantec's manger of corporate public relations, initially declined to reply. 'There are legitimate reasons for not giving blanket guarantees--one of those is a court order,' he said at first. 'There are extenuating circumstances and gray issues.'" Declan McCullagh and Anne Broache, *Will security firms detect police spyware?*, CNET NEWS,

## B. Mobile phones as roving bugs

News reports in 2006 revealed that the FBI is able to remotely enable the microphones of mobile phones. Using this technique, described as a 'roving bug' in court documents, the FBI remotely instructs a mobile phone to turn on its microphone, and then silently transmits the recorded audio back to the government's remote servers, all without notifying the user.[124] The feature has been used against two alleged mafia kingpins, who had been careful to avoid saying anything incriminating when making calls using their mobile phones.[125] They were not so careful when they believed that the phones were off.

While it is unclear how the government is able to remotely enable the microphones, most experts point to a software update of some kind.[126] If an update is used, it is also unclear how the software is being covertly installed onto the suspect's phone – that is, if the government is exploiting an un-patched vulnerability in the phone's software,[127] or if government agencies have been able to obtain the assistance of wireless phone companies or the device manufacturers themselves – most of whom have refused to discuss the matter.[128]

---

July 17, 2007, (page 2) *available at* http://news.cnet.com/Will-security-firms-detect-police-spyware---page-2/2100-7348_3-6197020-2.html

[124] "The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations … Nextel and Samsung handsets and the Motorola Razr are especially vulnerable to software downloads that activate their microphones, said James Atkinson, a counter-surveillance consultant who has worked closely with government agencies. 'They can be remotely accessed and made to transmit room audio all the time,' he said. 'You can do that without having physical access to the phone.'" Declan McCullagh, FBI *taps cell phone mic as eavesdropping tool*, ZDNET, December 1, 2006, *available at* http://news.zdnet.com/2100-1035_22-150467.html.

[125] "Nextel cell phones owned by two alleged mobsters, John Ardito and his attorney Peter Peluso, were used by the FBI to listen in on nearby conversations. The FBI views Ardito as one of the most powerful men in the Genovese family, a major part of the national Mafia." Declan McCullagh, FBI *taps cell phone mic as eavesdropping tool*, ZDNET, December 1, 2006, *available at* http://news.zdnet.com/2100-1035_22-150467.html.

[126] "But other experts thought microphone activation is the more likely scenario, mostly because the battery in a tiny bug would not have lasted a year and because court documents say the bug works anywhere "within the United States"--in other words, outside the range of a nearby FBI agent armed with a radio receiver. In addition, a paranoid Mafioso likely would be suspicious of any ploy to get him to hand over a cell phone so a bug could be planted. And Kolodner's affidavit seeking a court order lists Ardito's phone number, his 15-digit International Mobile Subscriber Identifier, and lists Nextel Communications as the service provider, all of which would be unnecessary if a physical bug were being planted." Declan McCullagh, FBI *taps cell phone mic as eavesdropping tool*, ZDNET, December 1, 2006, *available at* http://news.zdnet.com/2100-1035_22-150467.html.

[127] See, for example, Collin Mulliner and Charlie Miller, *Injecting SMS Messages into Smart Phones for Security Analysis*, In the Proceedings of the 3rd USENIX Workshop on Offensive Technologies Montreal, Canada August 2009, *available at* http://www.usenix.org/events/woot09/tech/full_papers/mulliner.pdf.

[128] "Verizon Wireless said only that it 'works closely with law enforcement and public safety officials. When presented with legally authorized orders, we assist law enforcement in every way possible.' A Motorola representative said that 'your best source in this case would be the FBI itself.' Cingular, T-Mobile, and the CTIA trade association did not immediately respond to requests for comment." Declan McCullagh, FBI *taps cell phone mic as eavesdropping tool*, ZDNET, December 1, 2006, *available at* http://news.zdnet.com/2100-1035_22-150467.html.

### C. In-car navigation systems

In 2003, the 9th Circuit Court of Appeals ruled that providers of in-car navigational/GPS services can be forced to secretly enable the microphones in a suspect's car without the person's knowledge and remotely wiretap them.

This case relates to in-car navigation systems with built in cellular data service, and the government's attempt to turn these devices into roving bugs. These products generally enable a customer to press a button in their vehicle to call for help whenever they get lost, and further include added safety functionality – such as the ability automatically call an ambulance whenever the car has an accident.[129] These devices are typically pre-installed by car manufacturers, who also install microphones in the vehicles – permitting the customer to speak to call center workers when their assistance is needed.

While there was little to be gained by wiretapping a customer's calls to the emergency response call center staff, the FBI took an interest in the microphones pre-installed in many luxury vehicles, and the cellular transmission capabilities of the in-car navigational systems. In this case, FBI agents sought to covertly enable microphones without the suspects' knowledge, and then use the existing cellular capabilities in the system to listen in on in-car conversations.[130]

The FBI agents obtained a valid intercept order from the district court directing The Company[131] to provide the necessary assistance to wiretap the suspects. In making its argument as to why it should not have to comply with the court's order, The Company cited the legislative history of the Communications Privacy Act of 1996, which it claimed prohibits wiretap orders that "require a company to actually accomplish or perform the wiretap" or where "wiretap activity take place on …. company premises."[132] The court dismissed this argument, contrasting between telephone wiretaps mentioned in the Congressional Record in which "law enforcement is familiar with the technology and

---

[129] "The System automatically contacts the Company if an airbag deploys or the vehicle's supplemental restraint system activates." See: In the Matter of the Application of the UNITED STATES FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL COMMUNICATIONS, The Company v. UNITED STATES of America, 349 F.3d 1132.

[130] "Upon request by the FBI, the district court issued several ex parte orders pursuant to 18 U.S.C. § 2518(4), requiring the Company to assist in intercepting oral communications occurring in a certain vehicle equipped with the System." See: In the Matter of the Application of the UNITED STATES FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL COMMUNICATIONS, The Company v. UNITED STATES of America, 349 F.3d 1132.

[131] OnStar is the most well known of these in-car navigational services. While the identity of The Company who brought this case was never revealed by the court, "[c]ourt records strongly point to OnStar's Texas-based competitor ATX Technologies, which makes the 'Tele Aid' systems used in Mercedes vehicles: the description fits the Tele Aid systems, and the Dallas-based attorney listed as arguing the appeal is also representing ATX in unrelated civil litigation in Texas. ATX spokesman Gary Wallace said he couldn't immediately comment." Kevin Poulsen, *Court limits in-car FBI spying*, SECURITYFOCUS, November 19, 2003, *available at* http://www.securityfocus.com/print/news/7491.

[132] "[Title III] should not be construed as authorizing issuance of an order for land line telephone company assistance which either requires a company to actually accomplish or perform the wiretap or requires that law enforcement wiretap activity take place on land line telephone company premises." S.Rep. No. 99-541, at 29-30 (1986).

needs only access to wires remote from the carrier's premises" and the in-car microphone example, where "the FBI cannot intercept communications in the vehicle without the Company's `facilities [or] technical assistance.'"[133]

The Court disagreed, stating that it believed that the FBI certainly has the legal authority to order firms to turn their own technology against their customers. However, the FBI's requests were still ruled to be invalid. Pointing to the *minimum of interference* language in 18 USC §2518, the Court stated that "the obligation of private citizens to assist law enforcement, even if they are compensated for the immediate costs of doing so, has not extended to circumstances in which there is a complete disruption of a service they offer to a customer as part of their business." Due to the fact that The Company's ability to provide services to customers under surveillance was severely restrained,[134] the Court ruled that the FBI's order was improper.

While the 9th Circuit's decision protected customer privacy in this particular case, the Court left a clear path for compelled assistance with covert surveillance if doing so does not hinder a company's ability to provide service to its customers. If anything, this rather hollow victory for the privacy community was actually a win for the government.

### D. Torrentspy

In 2006, Torrentspy, a popular peer-to-peer filesharing search engine was taken to court by the Motion Picture Association of America (MPAA). Torrentspy had pro-actively disabled the logging of any data on its visitors, so that if compelled to, it would be unable to provide any information identifying its users. The company had also inserted clear language in its privacy policy to inform its users that it would not monitor their activity without their consent.[135]

In May of 2007, the MPAA convinced a federal judge to force TorrentSpy to enable logging on its servers – that is, to modify the code running on its servers in order to capture IP address information on its visitors. The judge relied upon

---

[133] "In contrast to standard land line wiretaps, the FBI cannot intercept communications in the vehicle without the Company's 'facilities [or] technical assistance.' Since such hands-on assistance is necessary, assistance may be mandated by an order under § 2518(4). *Cf.* S.Rep. No. 99-541, at 29 (recognizing that cellular service providers allow law enforcement to use their premises and that Congress did not intend to alter this arrangement with any of its 1986 amendments to title III)." See: In the Matter of the Application of the UNITED STATES FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL COMMUNICATIONS, The Company v. UNITED STATES of America, 349 F.3d 1132.

[134] "In this case, FBI surveillance completely disabled the monitored car's System. The only function that worked in some form was the emergency button or automatic emergency response signal. These emergency features, however, were severely hampered by the surveillance: Pressing the emergency button and activation of the car's airbags, instead of automatically contacting the Company, would simply emit a tone over the already open phone line. No one at the Company was likely to be monitoring the call at such a time, as the call was transferred to the FBI once received. There is no assurance that the FBI would be monitoring the call at the time the tone was transmitted; indeed, the minimization requirements …. preclude the FBI from listening in to conversations unrelated to the purpose of the surveillance. Also, the FBI, however well-intentioned, is not in the business of providing emergency road services, and might well have better things to do when listening in than respond with such services to the electronic signal sent over the line. The result was that the Company could no longer supply any of the various services it had promised its customer, including assurance of response in an emergency." See: In the Matter of the Application of the UNITED STATES FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL COMMUNICATIONS, The Company v. UNITED STATES of America, 349 F.3d 1132.

[135] "TorrentSpy.com will not collect any personal information about you except when you specifically and knowingly provide such information." See: TorrentSpy Privacy policy, available at: http://web.archive.org/web/20070410082408/http://www.torrentspy.com/privacy.asp

the fact that the IP address information is available in computer memory, if just for a few seconds, as evidence that the information is "stored" and thus the company could be compelled to store it.[136]

Demonstrating a level of *chutzpah* common amongst those in the BitTorrent business,[137] TorrentSpy thumbed its nose at the judge's order, and simply blocked all US visitors from accessing the site,[138] citing an "uncertain legal climate in the US regarding user privacy and an apparent tension between US and European Union privacy laws."[139]

## E. Hushmail

Since 1999, Hush Communications, a Canadian technology company, has offered consumers a free Web-based encrypted email service.[140] In contrast to the free email solutions provided by Microsoft's Hotmail and Yahoo, Hush's Communication's Hushmail product enables users to compose, transmit and receive encrypted email using an encryption key only known to the user. By using this service, a user can securely communicate with another Hushmail user, or one of the hundreds of thousands of existing users of OpenPGP compatible encryption tools.

While Hushmail's own marketing materials promised users absolute privacy,[141] a drug-related court case proved otherwise. In 2007, Hush received an order from the Supreme Court of British Columbia in response to a Mutual Legal Assistance Treaty request by the US Drug Enforcement Agency (DEA). US court documents reveal that Hush provided the plain-text contents of three users' email accounts to DEA agents.[142]

At the time, Hushmail offered two different forms of encrypted webmail. In the default mode, the user would type her encryption password into a Web form, that would be transmitted to Hush's servers, which would in turn decrypt the email, and then transmit the plaintext of the email to the user. A second more secure solution provided users with a Java-based applet, which downloaded the encrypted mail from Hush's servers, and then decrypted the emails locally. This latter approach provided significantly more security, since the password never left the user's computer, and the decrypted emails never touched Hush' servers or were transmitted over the Internet in the clear.

In this particular case, media reports indicate that the suspects were using the more lightweight of the two encryption solutions, in which a user's password was transmitted to and temporarily stored on Hush's servers for the

---

[136] Eric Bangeman, *Judge: TorrentSpy must preserve data in RAM*, ARS TECHNICA, August 28, 2007, *available at* http://arstechnica.com/tech-policy/news/2007/08/judge-torrentspy-must-preserve-data-in-ram.ars.

[137] See generally various mocking emails in response to DMCA takedowns, http://thepiratebay.org/legal

[138] Of course, if no US residents could interact with the website, then there would be no data that would need to be retained. As a result, Torrentspy did not necessarily violate the judge's order.

[139] See: http://web.archive.org/web/20070831074431/http://www.torrentspy.com/US_Privacy.asp

[140] Hushmail's free service has a limit of 2MB storage per account, and offers a premium pay service with much higher storage capacity.

[141] "Hushmail, a longtime provider of encrypted web-based email, markets itself by saying that 'not even a Hushmail employee with access to our servers can read your encrypted e-mail, since each message is uniquely encoded before it leaves your computer.'" Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED NEWS – Threat Level, November 7, 2007, *available at* http://www.wired.com/threatlevel/2007/11/encrypted-e-mai.

[142] See: http://www.wired.com/images_blogs/threatlevel/files/steroids.source.prod_affiliate.25.pdf

process of mail decryption.[143] Pursuant to the court order, Hush modified their product to capture the passwords of the three suspects, which it then used to decrypt the 12 CDs worth of email that it provided to US law enforcement agents.[144]

While the Java-based solution would have protected users against this particular form of government compelled circumvention of data encryption, it is by no means foolproof. Just as the company was compelled to modify the programs that ran on its own servers, it could just as easily be compelled to create a modified version of its Java tool which would steal the user's password.[145] Once news of Hush's compliance with the court order became public, Phil Zimmerman, the original designer of Pretty Good Privacy (PGP) and a member of Hush Communication's Advisory Board defended the company, telling one journalist that:

> "If your threat model includes the government coming in with all of force of the government and compelling service provider to do things it wants them to do, then there are ways to obtain the plaintext of an email. Just because encryption is involved, that doesn't give you a talisman against a prosecutor. They can compel a service provider to cooperate …. It would be suicidal for [Hush's] business model if they [ignored court orders] …. there are certain kinds of attacks that are beyond the scope of their abilities to thwart. They are not a sovereign state."

### F. Skype in China

Most of the examples we have of service providers being forced into inserting back doors related to the surveillance of specific individuals. This is not the only model for the use of backdoors. As this example will demonstrate, sometimes these can be used against an entire population, rather than a few individuals being targeted by an investigation.

---

[143] "The rub of that option is that Hushmail has — even if only for a brief moment — a copy of your passphrase. As they disclose in the technical comparison of the two options, this means that an attacker with access to Hushmail's servers can get at the passphrase and thus all of the messages." Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED NEWS – Threat Level, November 7, 2007, *available at* http://www.wired.com/threatlevel/2007/11/encrypted-e-mai.

"The only way to decrypt encrypted Hushmail messages stored on our servers is with the private keys associated with the senders and recipients of those messages, and the only way to access those private keys is with the associated passphrases. …. The key point, though, is that in the non-Java configuration, private key and passphrase operations are performed on the server- side. This requires that users place a higher level of trust in our servers as a trade off for the better usability they get from not having to install Java and load an applet." Email from Hush CTO Brian Smith to Wired News Reporter Kevin Poulsen: http://blog.wired.com/27bstroke6/hushmail-privacy.html

[144] "In the case of the alleged steroid dealer, the feds seemed to compel Hushmail to exploit this hole, store the suspects' secret passphrase or decryption key, decrypt their messages and hand them over." Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED NEWS – Threat Level, November 7, 2007, *available at* http://www.wired.com/threatlevel/2007/11/encrypted-e-mai.

[145] "[Hushmail's CTO] concurs and hints that Hushmail's Java architecture doesn't technically prohibit the company from being able to turn over unscrambled emails to cops with court orders … The extra security given by the Java applet is not particularly relevant, in the practical sense, if an individual account is targeted.**"** Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED NEWS – Threat Level, November 7, 2007, *available at* http://www.wired.com/threatlevel/2007/11/encrypted-e-mai.

In the United States, technology companies are for the most part free to offer their products without the requirement to build in surveillance capabilities at the design stage.[146] Unfortunately, this is not the case everywhere in the world, with China being perhaps the most aggressive in this area.

Skype is a popular voice-over-IP software program that lets users make free peer-to-peer phone calls and conduct instant messaging over the Internet. In order to gain a foothold into the Chinese market, Skype partnered with TOM Online, a leading Chinese provider of wireless phone services, and in 2005 released a special version of the Skype software, known as TOM-Skype.[147] The following year, the company publically admitted that the TOM-Skype client contains a filtering mechanism that prevents users from sending text messages that include banned phrases such as "Falungong" and "Dalai Lama." Defending the practice, Niklas Zennström, the company's CEO told one reporter that the company is merely complying with local law which, "is what everyone else in that market is doing. "[148] While human rights groups were not particularly happy with Zennström's justification, his statement is true: Microsoft, Yahoo and Google have all built censorship technologies into the products they deliver to the Chinese market, and all have defended their behavior by stating that they are required to do so by law.[149]

In addition to the censorship filtering code, human rights groups also claimed that the TOM-Skype contains Trojan horse capabilities that can be used for surveillance by the Chinese Government.[150] These claims were vigorously denied by Skype, which proclaimed that "if the message is found unsuitable for displaying, it is simply discarded and not displayed or transmitted anywhere," "the text filter does not affect in any way the security and encryption

---

[146] The exception to this rule, of course, is the CALEA mandated surveillance capabilities, required of all telecommunication providers. The government has attempted to apply this law to other markets, but does not appear to have had much success.

[147] "In a move to carve out a chunk of China's nascent market for Internet telephone services, Skype Technologies has expanded its partnership with Beijing-based Tom Online by creating a joint venture that will develop and deliver premium services. Building on their agreement last year to develop a simplified version of the Skype VoIP (voice over Internet Protocol) software in Chinese, the companies plan to offer a number of services that customers can use for a fee." John Blau, Skype, *Tom Online to launch Chinese joint venture,* INFOWORLD, September 06, 2005, *available at* http://www.infoworld.com/t/networking/skype-tom-online-launch-chinese-joint-venture-026.

[148] "Skype, the fast-growing internet communications company that belongs to Ebay, has admitted that its partner in China has filtered text messages, defending this compliance with censorship laws as the only way to do business in the country. In a Financial Times interview, Niklas Zennström, Skype's chief executive, responded to accusations that the company had censored text messages containing words like "Falun Gong" – a banned movement – and "Dalai Lama". He said that Tom Online, its joint venture partner in China, was complying with local law." Alison Maitland, *Skype says texts are censored by China*, FINANCIAL TIMES, April 18, 2006, *available at* http://www.ft.com/cms/s/2/875630d4-cef9-11da-925d-0000779e2340.html.

[149] Human Rights Watch, *How Multinational Internet Companies assist Government Censorship in China*, Chapter in "Race to the Bottom" Corporate Complicity in Chinese Internet Censorship, August 8, 2006, *available at* http://www.hrw.org/reports/2006/china0806/5.htm#_Toc142395828.

[150] "Dynamic Internet Technologies (DIT), a North America-based company known for its products that override Internet censorship, recently discovered that the Internet phone service company Skype is cooperating with Internet censorship in China. On Monday DIT announced that it has tested and confirmed that Skype.com redirects visits from Chinese IP addresses to the homepage of Tom-Skype that has Trojan horse capabilities." *Skype Strengthens Cooperation with Chinese Regime On Internet Censorship*, THE EPOCH TIMES, September 29, 2007, *available at* http://en.epochtimes.com/news/7-9-29/60228.html.

mechanisms of Skype", "full end-to-end security is preserved and there is no compromise of people's privacy" and "calls, chats and all other forms of communication on Skype continue to be encrypted and secure."[151]

In 2008, a group of Canadian human-rights activists and computer security researchers discovered that in addition to censoring messages, the TOM-Skype software also transmits these flagged messages as well as information identifying the sender and recipient back to one of several TOM-Skype run servers in mainland China. The researchers were able to download and analyze copies of the surveillance data from the TOM-Skype servers, because the Chinese computers were improperly configured, leaving the log files accessible to anyone with a Web browser who knew their location. In just two months, the servers archived more than 166,000 censored messages from 44,000 users.[152]

Once news of the surveillance became public, Skype's President revealed that "we have discovered in our conversations with TOM is that they in fact were required to do this by the Chinese government" and that the firm would "ensure that it is clear and transparent to Skype users that their chat messages into and out of China may be monitored and stored."[153] The company did, however, quickly password protect the surveillance servers, so that the logs of individuals' conversations were no longer publicly accessible.[154]

### G. The Java Anonymous Proxy

All of the preceding examples relate to the government gaining access to or circumventing the privacy protections in commercial services, it appears that legal coercion can similarly be used to sneak backdoors into open source software products.[155]

There are now several open source software projects which aim to provide end-users with the ability to anonymously browse the Internet. While Tor[156] is perhaps the most well known of these, others do exist, including the Java Anonymous Proxy (JAP), a software tool designed by researchers from several German universities. Each anonymous networking system is designed differently, but in general, they all provide users with privacy by bouncing their encrypted Internet traffic through several servers around the world. Ideally, a government watching a suspect's network connection will not be able to learn which Web sites she is visiting, while the owners of those Web sites will not be able to identify the true IP address of the anonymous visitor.

---

[151] See: Jaanus Kase, *Comments about Skype chat text filtering in China* , Post to Official Skype Blog, April 19, 2006, *available at* http://share.skype.com/sites/en/2006/04/comments_about_skype_chat_text.html.

[152] See: John Markoff, *Surveillance of Skype Messages Found in China*, NEW YORK TIMES, October 1, 2008, *available at* http://www.nytimes.com/2008/10/02/technology/internet/02skype.html?pagewanted=all

[153] Josh Silverman, *Answers to some commonly asked questions about the Chinese privacy breach*, Post to Official Skype Blog, October 4, 2008, *available at* http://share.skype.com/sites/en/2008/10/answers_to_some_commonly_asked.html.

[154] "We also learned yesterday about the existence of a security breach that made it possible for people to gain access to those stored messages on TOM's servers. We were very concerned to learn about both issues and after we urgently addressed this situation with TOM, they fixed the security breach." John Silverman, *Skype President Addresses Chinese Privacy Breach*, Post to Official Skype Blog, October 2, 2008, *available at* http://share.skype.com/sites/en/2008/10/skype_president_addresses_chin.html.

[155] See: Ken Coar, *The Open Source Definition*, Open Source Initiative, July 24, 2006, *available at* http://www.opensource.org/docs/definition.php.

[156] See: The Tor Project, *available at* http://www.torproject.org.

In mid 2003, the JAP network went down "due to a hardware failure." When the service was restored, users were informed that they had to install an "upgraded version" of the application in order to again use the anonymizing network. No explanation was given for the necessary upgrade. However, since JAP was an open source project, users could look through the source code and quickly determine which lines of code in had been added to the latest version. Savvy users quickly discovered a few suspicious looking lines of source code:

> "CAMsg::printMsg(LOG_INFO,"Loading Crime Detection Data....\n");"
>
> "CAMsg::printMsg(LOG_CRIT,"Crime detected - ID: %u - Content: \n%s\n",id,crimeBuff,payLen);"[157]

When confronted by members of the security community, the JAP developers acknowledged the existence of the "crime detection function" in the system, and revealed that the code had been inserted in response to a court order obtained by the German Federal Office of Criminal Investigation. They pledged that privacy in the JAP system was safe, because only "one Web site [was] currently being disclosed, and only under court-ordered monitoring."[158]

This revelation resulted in a significant amount of criticism from members of the academic security community, as well as multiple negative articles in the press. While the JAP developers were merely complying with the court's order, they still suffered significant damage to their project's reputation. According to a statement by the developers in 2006, only one court order has ever been issued forcing them to use the backdoor.[159]

## V. The law

While these examples clearly demonstrate that governments have forced service providers to insert back doors into their own products, the legal justification requiring the company to comply is not always clear. Often, the public only learn of the company's assistance to the government through a brief mention in court documents. However, the legal documents presented to the company are rarely if ever made public. There are several laws which can be used to justify the compelled insertion of back doors in products. These areas of US law will now be highlighted.

---

[157] Thomas C. Greene, Net anonymity service back-doored, THE REGISTER, August 21, 2003, available at http://www.theregister.co.uk/2003/08/21/net_anonymity_service_backdoored/.

[158] "Except for the case mentioned above, the protection of the users' anonymity is and will remain the central warranty of AN.ON. The AN.ON operators warn against the generalisation of this single case and the general jeopardising of the whole service. Anonymity in the internet makes still sense when the access to a single website with illegal content is recorded for a limited time period due to a court decision." *AN.ON still guarantees anonymity*, Press Release, August 19, 2003, available at https://www.datenschutzzentrum.de/material/themen/presse/anonip_e.htm.

[159] "In 2006, there has been only one single surveillance court order to single Mix operators. A few exactly specified web addresses were affected. The observation has been stopped after the court order expired (one month). " *JAP and Crime Prevention*, *available at* http://anon.inf.tu-dresden.de/strafverfolgung/index_en.html.

### A. The Wiretap Act (Title III)

The Wiretap Act[160] regulates the collection of actual content of wire and electronic communications. The Wiretap Act was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally known as "Title III." Prior to the 1986 amendment by Title I of the Electronic Communications Privacy Act (ECPA), it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications.[161]

18 U.S.C. §§ 2518(4) states that:

> An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person **shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception** unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.

18 U.S.C. §§ 2518(4) also states that:

> Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.

In the car navigation case discussed earlier in this article, the court determined that the term "other person" in 18 U.S.C. §§ 2518(4) also includes "an individual or entity who both provides some sort of service to the target of the surveillance and is uniquely situated to assist in intercepting communications through its facilities or technical abilities." At least based that court's interpretation of the law in that case, the Wiretap Act can be used to justify forcing a service provider to create new functionality in its products solely for the purpose of wiretapping customers.

While the technical details of the FBI's Magic Lantern/CIPAV system have yet to be revealed, some legal experts did discuss the possible means through which the government might be able to compel anti-virus vendors to ignore or even white list the FBI's spyware tool. An attorney with the Electronic Frontier Foundation told one journalist that "[t]he government would be pushing the boundaries of the law if it attempted to obtain such an order … There's simply no precedent for this sort of thing." He did, however, point to the Wiretap Act as one possible source for this coercive power, adding that "[t]here is some breadth in that language that is of concern and that the Justice Department may attempt to exploit."[162]

---

[160] Codified in 18 U.S.C. §§ 2510-2522.

[161] http://ilt.eff.org/index.php/Privacy:_Wiretap_Act

[162] Declan McCullagh and Anne Broache, *Will security firms detect police spyware?*, CNET NEWS, July 17, 2007, (page 2) *available at* http://news.cnet.com/Will-security-firms-detect-police-spyware---page-2/2100-7348_3-6197020-2.html

### B. *United States v. New York Telephone Co. (1977)*

One of the most relevant cases relating to compelled covert assistance is that of *United States v. New York Telephone Co.* In this case, the District Court authorized the FBI to install and use pen register surveillance devices[163] on two telephones used by the suspects of a government investigation. The court also directed the telephone company to furnish the FBI "all information, facilities and technical assistance" necessary to install and use the devices. The telephone company refused to lease to the FBI phone lines that were needed for unobtrusive installation of the pen registers, and thereafter asked the court to vacate that portion of the pen register order directing respondent to furnish facilities and technical assistance to the FBI on the ground that such a directive could be issued only in connection with a Title III wiretap order.

The Court of Appeals held that the District Court abused its discretion in ordering the telephone company to assist in installing and operating the pen registers, and expressed concern that such a requirement could establish an undesirable precedent for the authority of federal courts to impress unwilling aid on private third parties.

The Supreme Court was far more willing to extend these coercive powers to the US government, looking primarily to the All Writs Act. That Act states:

> "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[164]

With regard to this case, first, the Supreme Court noted that "[t]he assistance of the Company was required … to implement a pen register order which … the District Court was empowered to issue." It also noted that "without the Company's assistance there is no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished … The provision of a leased line by the Company was essential to the fulfillment of the purpose -- to learn the identities of those connected with the gambling operation -- for which the pen register order had been issued."

Then, citing the All Writs Act, the court ruled that "[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it."[165] Furthermore, "The power conferred by the [All Writs] Act extends, under appropriate circumstances, to persons who (though not parties to the original action or engaged in wrongdoing) are in a position to frustrate the implementation of a court order or the proper administration of justice. Here respondent … was not so far removed as a third party from the underlying controversy that its assistance could not permissibly be compelled by the order of the court based on a probable cause showing that respondent's facilities were being illegally used on a continuing basis."

Concluding, the court wrote that "[t]he conviction that private citizens have a duty to provide assistance to law enforcement officials when it is required is by no means foreign to our traditions."[166] However, in an effort to place at least some limit to this power, the court noted that the District Court's original order "required minimal effort on the part of the Company and *no disruption to its operations.*"

---

[163] Pen register devices record the numbers dialed by a phone, without overhearing oral communications or indicating whether calls are completed.

[164] 28 U.S.C. § 1651(a).

[165] *Adams v. United States ex rel. McCann*, 317 U. S. 269, 317 U. S. 273 (1942).

[166] 434 U.S. at 175 n. 24, 98 S.Ct. 364.

### C. Other mentions of the All Writs Act

While *New York Telephone* is the most important case that relies on the All Writs Act to justify these coercive powers, it is not the only time that the Government has depended upon this age-old statute.

In a 2005 case relating to attempts by the government to obtain the real time location information of mobile phone customers, the Department of Justice revealed that:

> "Currently, the government routinely applies for and upon a showing of relevance to an ongoing investigation receives 'hotwatch' orders issued pursuant to the All Writs Act. Such orders direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of investigation immediately after the issuer records that transaction.
>
> While the evidence sought by All Writs orders in such cases is often pre-existing, see, e.g., United States v. Doe, 537 F. Supp. at 839 (ordering disclosure of 6 prior months of telephone toll records), there is no legal impediment to issuing such an order for records yet to be created. See, e.g., In re Application of the U.S.A. For An Order Directing X To Provide Access to Videotapes, 2003 WL 22053105, No. 03-89 (Aug. 22, 2003 D. Md.) (directing that production of subsequently-created videotapes made by security camera installed in apartment hallway)."[167]

In the same case, the Department of Justice noted that the power to issue supplemental orders in aid of the court's jurisdiction "extends to persons who are not defendants and have not obstructed justice."[168] Again, for this authority, the Department of Justice turned to the All Writs Act:

> "[A]ny additional authority needed for the Court to direct prospective disclosure of cellsite information, the Court already possesses it under the All Writs Act … which authorizes the issuance of orders in aid of the Court's jurisdiction."

The Judge in this case disagreed with the Department of Justice, denying their request, and ruled that:

> "The government thus asks me to read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching and detailed statutory scheme that has received the legislature's intensive and repeated consideration. Such a broad reading of the statute invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority."[169]

---

[167] Letter from Department of Justice, *In re Application For Pen Register and Trap and Trace Device With Cell Site Location Authority*, Magistrate's Docket No. 05-1093(JO), October 11, 2005, *available at* http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_govt_reply.pdf.

[168] United States v. Doe, 537 F. Supp. 838 (E.D.N.Y. 1982)

[169] Kurt Opsahl, *All Writs Redux*, post to Deep Links blog, Electronic Frontier Foundation, October 26, 2005, *available at* http://www.eff.org/deeplinks/2005/10/all-writs-redux.

The government's attempt to turn the All Writs Act into the "All Surveillance Act" appears to have been frustrated, at least in this case.[170] However, it also seems that its argument has been repeatedly (and successfully) used to justify the issuance of credit card "hotwatch" orders.[171]

### D. The Foreign Intelligence Surveillance Act (FISA)

While both the Wiretap Act and the All Writs Act seem to be the legal tools of choice for law enforcement agencies, there is at least one other legal avenue through which the government can force service providers to insert backdoors into their own products. The 2008 Protect America Act amended the Foreign Intelligence Surveillance Act[172] to state that:

> "The Director of National Intelligence and Attorney General may direct a person to …. immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that such person is providing to the target … The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to subsection (e)."[173]

Details on the government's interpretation and use of this law are understandably impossible to find. However, some commentators have argued that the law gives "the government wide powers to order communication service providers such as cell phone companies and ISPs to make their networks available to government eavesdroppers."[174]

## VI. Encryption can be circumvented

Let us now go back to our earlier hypothetical scenario in which all cloud services have switched to data encryption with a key private to the user. In this situation, the government will not be able to use a subpoena to force the revelation of a user's private files, since the service provider will only possess encrypted data. However, it may be possible for the government to force that company to place a backdoor in its web based product in order to steal the user's encryption key. As an example, when the user enters her password in to the encryption enhanced Google Docs web application, instead of keeping the password in local memory on her computer, a copy of it will be silently recorded and later transmitted to a FBI server.

While market forces might be able to neutralize the privacy problems associated with the third party doctrine by encouraging the use of encryption, there are no readily available market forces or technology that can protect a

---

[170] Kurt Opsahl, *The All Surveillance Act*, post to Deep Links blog, Electronic Frontier Foundation, October 12, 2005, *available at* http://www.eff.org/deeplinks/2005/10/all-surveillance-act.

[171] This author has attempted to find out more about these prospective requests for credit card transaction information. The US Department of Justice found 10 relevant documents in response to the author's Freedom of Information Act request, but has refused to deliver them.

[172] 50 USC 1566.

[173] 50 USC 1805b (f).

[174] Ryan Singel, *Analysis: New Law Gives Government Six Months to Turn Internet and Phone Systems into Permanent Spying Architecture – UPDATED*, WIRED NEWS – Threat Level, August 6, 2007, *available at* http://www.wired.com/threatlevel/2007/08/analysis-new-la.

company from a lawful order compelling that firm to insert a backdoor into its own products. To make matters worse, the move to cloud computing increases the amount of private information available at risk of covert government capture, and, as this next section will explain, also makes it significantly easier for companies to deploy these compelled backdoors.

### A. Traditional software is pretty hard to covertly back door

One of the defining features of the Internet era is the ability of technology firms to later fix problems in their products, to release new features after the date of initial sale, and in some cases, to even remove useful features.[175] A fix that would in years past have required a costly and slow product recall can now be deployed to all customers with a mere software update. This ability to release products half-finished, rushing them to the market confident in the knowledge that remaining issues can be fixed with a later patch has led to a situation that some experts call a state of perpetual beta.[176]

In many cases, these updates must be manually downloaded and installed by the user. When this is the case, adoption rates can be extremely low.[177] This can lead to problems for government agencies that wish to compel a traditional software company, such as an operating system vendor, into creating and deploying a back door. If users cannot be convinced to download and install critical security updates that might protect them from hackers, how can they be convinced to download and install government back doors that will pilfer their private files.

---

[175] "A federal court in Marshall, Texas, ordered EchoStar Communications, the second-largest satellite TV operator in the United States, to disable the digital video recorders currently being used by millions of its customers. EchoStar, which has more than 12 million customers, has been ordered to disable the DVRs within 30 days." *TiVo's Day: EchoStar DVRs Off*, Red Herring, August 17, 2006, *available at* http://www.redherring.com/Home/18034. "Apple is clamping down on piracy by imposing restrictions on the way that music can be shared via the iTunes service. Changes to the service stop people listening across the internet to playlists of songs created by others." *Apple iTunes update irritates fans*, BBC NEWS, May 29, 2003, *available at* http://news.bbc.co.uk/2/hi/technology/2946180.stm. "In iTunes 4.5, you can authorize up to five Macs or Windows computers to play your purchased music -- up from three. But Apple giveth and Apple taketh away: you can now burn a playlist containing purchased music up to seven times (down from ten). And the old workaround of simply changing the playlist slightly does not work." Jason Schultz, *Meet The New iTunes, Less than the Old iTunes?,* post to LawGeek blog, April 29, 2004, *available at* http://lawgeek.typepad.com/lawgeek/2004/04/meet_the_new_it.html. "However, Apple has moved to restrict the streaming capability. In the good old days it used to support five simultaneous listeners, but now allows only allows five listeners a day." Nick Farrell, *Apple squeezes iTunes customers*, THE INQUIRER, March 16, 2005, *available at* http://www.theinquirer.net/inquirer/news/156/1002156/apple-squeezes-itunes-customers.

[176] "The open source dictum, 'release early and release often' in fact has morphed into an even more radical position, 'the perpetual beta,' in which the product is developed in the open, with new features slipstreamed in on a monthly, weekly, or even daily basis. It's no accident that services such as Gmail, Google Maps, Flickr, del.icio.us, and the like may be expected to bear a 'Beta' logo for years at a time." Tim O'Reilly, What *Is Web 2.0,* online essay, September 30, 2005, *available at* http://oreilly.com/lpt/a/6228.

[177] "Our measurements prove that silent updates and little dependency on the underlying operating system are most effective to get users of Web browsers to surf the Web with the latest browser version … We recommend any software vendor to seriously consider deploying silent updates as this benefits both the vendor and the user, especially for widely used attack-exposed applications like Web browsers and browser plug-ins… With silent updates, the user does not have to care about updates and system maintenance and the system stays most secure at any time. We think this is a reasonable default for most Internet users." Thomas Duebendorfer and Stefan Frei, *Why Silent Updates Boost Security*, ETH Tech Report 302, May 05, 2009, *available at* http://www.techzoom.net/papers/browser_silent_updates_2009.pdf.

Another problem associated with the insertion of back doors in traditional software products is the fact that most vendors do not know their customers' identities. Many copies of Microsoft Windows and other software suites are bundled with new computers, negotiated as part of site licenses for companies and universities. Unless the user registers their software installation, the software supplier simply will not know which individual is associated with any particular computer. The widespread problem of software piracy makes this even worse, since these users are even less likely to register their illicit installations under their own names.

This inability to tie an identifiable customer to a particular software installation poses a serious barrier to the government's ability to compel most traditional software providers into rolling out covert back doors, even if the customer can be convinced to install it. Sure, the company can opt to supply to the sneaky update to *all* customers based on the assumption that the government's suspect will be one of the impacted users. However, this approach is likely to draw the attention of security researchers and hackers who routinely reverse engineer software updates in order to learn which flaws have been fixed.[178]

The move to cloud computing makes it far easier for the government to effectively force the deployment of covert back doors. This is due to a few key features specific to the Web 2.0 application model: identifiable customers, automatic, silent updates and the complete absence of visible product releases.

## B. Updates and the cloud

One of the most useful features of the Web 2.0 paradigm, for both provider and customer, is that users are always running the latest version of a particular Web based application. There is simply no need to coax an update, because it is simply impossible to run anything *but* the latest version.

The vast majority of cloud based software runs in a Web browser. In this model, a user visits a Web page, and her browser immediately downloads the programmatic code which is used to implement the Web page's functionality. When the user revisits that same Web site the next day, her Web browser requests the same content again, and then downloads it from the company's Web server.[179] If the Web site owner has updated the code, a new version of the application will be downloaded, without any notification to the user that the code running on her computer today is different than the day before.[180]

---

[178] "[A]utomatic patch-based exploit generation is possible as demonstrated by our experiments using 5 Windows programs that have recently been patched. We do not claim our techniques work in all cases or for all vulnerabilities. However, a fundamental tenet of security is to conservatively estimate the capabilities of attackers. Under this assumption, [automatic patch-based exploit generation] should be considered practical, and those who have received a patch should be considered armed with an exploit." David Brumley et al, *Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications*, Proceedings of the IEEE Security and Privacy Symposium, May, 2008, *available at* http://www.ece.cmu.edu/~dbrumley/pubs/apeg.pdf.

[179] In some cases, a cloud application might cache a local copy of its JavaScript code in the user's browser (such as with Gmail). However, this is only done for performance reasons – if the user clears his or her cache, uses a new computer, or if the application provider releases a new version of their software, the JavaScript code will be re-obtained. Likewise, there is no notification to the user that a cached copy is being used, or a new copy is being downloaded.

[180] "In response, Google asserted that its cloud-based system can quickly deploy upgrades and security updates to all of its customers, something that is less seamless when organizations maintain their own computer systems on site." David Sarno, *Los Angeles City Hall becomes tech giants' battlefield*, LOS ANGELES TIMES, September 28, 2009, *available at* http://www.latimes.com/business/la-fi-email-wars28-2009sep28,0,6817066,full.story.

Traditional software vendors, both application and operating system, ship software with a version number. Users can, if they know how, find out which version of Microsoft Word, Photoshop or Quicken they are running. In fact, many applications display their current version number when starting.

Contrast this to the situation for the users of cloud based services. Google does not provide a version number for its Gmail or Docs service. Neither does Yahoo, Facebook, or MySpace. New features might be announced, or suddenly appear, however, when bugs are fixed, these are usually done so quietly with no notification to the user.

If a user of Google Docs starts up her computer, connects to the Internet and accesses her documents, she has no way of knowing if her browser is executing different code than it ran the day before. The same user running Firefox or Microsoft Windows would have a much better chance of knowing this, and in most cases, of declining to perform an update if one was made available.

Finally, most cloud providers know a significant amount more about their customers than traditional software companies. Unless a customer has given a false name, email providers and social networking companies know who their customers are as well as the names and contact information for their friends. As a result, if law enforcement agencies serve a subpoena in order to obtain the files for a specific customer, most cloud computing providers know exactly which account to target.

This shift in the effectiveness of software updates and the ease of customer identification significantly weakens the ability of cloud providers to protect their customers' privacy with encryption. While Google could add encryption to its Docs application, the company could just as easily be forced to add a back door in to the browser code which would steal the user's key. As we have just explained, this would be automatically downloaded and executed the next time that the user logged in, with no way for her to avoid the update, or even know that it was applied. Furthermore, because of the fact that Google typically knows which *particular* user account an individual is using, it can issue the backdoor-laced update to only that user. Essentially, cloud computing makes it far easier for companies to force out covert backdoors with surgical precision to only those persons who the government has targeted.

## VII. Potential solutions to the compelled backdoor problem

The problem of compelled back doors is extremely difficult. Due to powers provided to the government by the various laws outlined earlier in this article, consumers can never completely trust the companies who make and supply the software that they use to go about their daily business online. Any firm can be compelled to insert a back door into its own product; no matter how committed it is to protecting the privacy of its customers.

The simplest solution to this problem would be to amend the law to prohibit this coercive behavior by government agencies. However, given the realities of Washington DC, and the fear of being accused of being soft on terrorism or child pornography, it is unlikely that Congress would agree to any form of legislative fix which took away this power. Thus, we focus our attention upon non-legislative solutions to this issue.

### A. Privacy through open source software

Of the backdoor examples presented in this article, most came to light through their mention in court documents, often in passing. Furthermore, while we know that *a* manufacturer of GPS navigation equipment was forced to snoop on its customers, six years on, we still do not know with certainty the identity of the company whose product was turned into a covert microphone by the FBI.

The *Java Anonymous Proxy* incident demonstrates that it is exceedingly difficult to covertly install a backdoor into an open-source software product, as inquisitive users will look through the changes in the source code with the intention of discovering the new feature. Furthermore, due to the highly distributed nature of many open source projects, even if developers in one country are forced into secrecy by a gag order, developers in another will not be. These developers will already be highly familiar with the source code, and thus will be most likely to notice and publicize any suspect changes.

Applying this observation to the market for cloud computing services, I argue that while the government could *in theory* force the Mozilla Corporation to insert a backdoor into its Weave encrypted browser add-on, such an action would likely be soon discovered. Whereas a court order could effectively lead to the circumvention of an encrypted cloud computing service provided by Google, Yahoo and Microsoft, I do not believe that the government's coercive powers are nearly as effective against open source software.

To slightly paraphrase Linus Torvalds, the creator of the Linux operating system, given enough eyeballs, all surveillance bugs are shallow.[181]

While open source products may provide superior protection from covert back doors, the current cloud computing market is primarily one in which consumers are provided free access to proprietary software. A switch to 100% open source is thus not likely to happen. Given the reality of the market, cloud software suppliers who do opt to embrace encryption should at least make sure that the programmatic code which has receives and makes use of each user's password be open source software – preferably the Web browser. As an example, Mozilla should provide a simple Application Programming Interface (API) through which cloud computing services can request the encryption and decryption of files – with the Firefox browser itself handling the user's password and all encryption functionality. This system design would provide the best of both worlds: increased protection for user's encryption keys and private files, while permitting private companies to continue to offer innovative technology through the propriety software model to which they are committed.

## B. Web application fingerprinting

As the Skype example demonstrates, it is far tougher to keep the backdoor in a piece of software a secret once it has been distributed to millions of users, especially if some of those users are security researchers. If backdoors are to remain secret, governments would be wise to take steps to deliver the compromised updates to only those suspects targeted by an investigation, rather than the population at large.

A problem that has long frustrated the academic security community is that users typically have no way to guarantee that the software running on their computers is safe, and has not been tampered with since it was released by the software vendor. Most of the efforts to address this issue have primarily focused on the authentication of software downloads and installations. However, these solutions do not address the threat of post-installation software modification.

The threat of post-installation modification of software has been partially addressed by file integrity tools such as Tripwire.[182] These applications examine the files on a system, and calculate an individual fingerprint (or "hash") for each file. Then, at regular intervals in the future, these fingerprints can be recalculated and compared to the

[181] http://en.wikipedia.org/wiki/Linus%27s_Law

[182] See generally, open source Tripwire, available at http://sourceforge.net/projects/tripwire/

previously created database. File integrity tools can play a key role in maintaining the security of a computer system, by providing system administrators with rapid notification after an improper change has been detected. Unfortunately, these tools are not commonly available to home users, although they are provided to businesses by some enterprise software vendors.[183]

The threat of secret backdoors in cloud based software is not one that can be fixed by authenticating the distribution of those web applications – since the back doors will be created and distributed by the web application provider. This risk essentially comes down to the fact that users of cloud based software have no real way of knowing if they are running the same piece of software that they were running the day before, or if the version they are running is different than that being used by their friends and colleagues. By providing users the ability to fingerprint and compare the web based applications they are running, we may be able to provide users some protection from cover backdoors – since, to avoid such a fingerprint-based scheme from flagging an individual software update, the vendor would need to distribute it to all users, and not just one individual targeted by a government investigation. Furthermore, as described earlier, back doors that are distributed to all users are far more likely to be discovered by curious security researchers than those distributed to a few individuals with care and precision.

There does not exist currently a software tool that enables users to compare the code of the web applications they are running to the code used by their friends, colleagues and the millions of other anonymous persons on the Internet. We do not believe that the design of such a system would be prohibitively difficult, and it could prove to be quite useful. Its creation is left as an exercise to others.

## VIII. Conclusion

As this article has noted, the mass adoption of cloud computing based services has significantly tipped the scales of privacy away from the end user – it is now much easier for hackers, private investigators or law enforcement and intelligence agents to access a user's private files. In some cases, these privacy risks are due to cost saving measures on the part of service providers. In others, the risks are due to the coercive powers wielded by the government.

Government agencies can now leverage economies of scale, and take advantage of the fact that the user no longer needs to be consulted or notified before her data is seized. In many cases, due simply to the reality that a single company is responsible for storing private data for millions of users, the government can obtain data on an additional individual at almost no cost. That is, the cost of adding one more person to the subpoena is free.

While the ease of government access made possible by the third party doctrine is certainly troubling, the use of data encryption and strict adherence to no-logging policies can act as a significant balance against this power. Were the third party doctrine to be done away with, the threats of hackers breaking into a company's servers and insiders peeking at a user's files would still remain – encryption is a technique that provides protection against all of these threats.

As we have documented at length, the real threat to end-user privacy is the ease with which the government can force an application provider to insert a backdoor or flaw in its own products. While this is certainly a risk that existed pre-cloud computing, it has been made more effective, and more difficult to discover through the shift to cloud-delivered software. The government can order a change, and the next day, every user of a service specified in the

[183] See generally, Sun Fingerprint Database, available at http://sunsolve.sun.com/show.do?target=content/content7

government's order will be running code with that backdoor – an efficiency of adoption that was never possible before. This is not an easy problem to solve, and the solutions we have proposed are by no means comprehensive. Until these or other solutions have been implemented and deployed, consumers should exercise significant caution when using cloud based tools to edit files that they wish to keep private.

In the cloud, the government is just one subpoena away.